EDUCATING THE EFFECTIVE DIGITAL FORENSICS PRACTITIONER: ACADEMIC, PROFESSIONAL, GRADUATE AND STUDENT PERSPECTIVES

By

Georgina Louise Humphries

Canterbury Christ Church University

Thesis submitted for the Degree of Doctor of Philosophy

2019

Dedication

This thesis is dedicated to my parents
and grandparents who have always
been a source of encouragement
and support.

Georgina Louise Humphries

October 2019

ABSTRACT

Over the years, digital forensics has become an important and sought-after profession where the gateway of training and education has developed vastly over the past decade. Many UK higher education (HE) institutions now deliver courses that prepare students for careers in digital forensics and, in most recent advances, cyber security. Skills shortages and external influences attributed within the field of cyber security, and its relationship as a discipline with digital forensics, has shifted the dynamic of UK higher education provisions. The implications of this now sees the route to becoming a digital forensic practitioner, be it in law enforcement or business, transform from on-the-job training to university educated, trained analysts. This thesis examined courses within HE and discovered that the delivery of these courses often overlooked areas such as mobile forensics, live data forensics, Linux and Mac knowledge. This research also considered current standards available across HE to understand whether educational programmes are delivering what is documented as relevant curriculum. Cyber security was found to be the central focus of these standards within inclusion of digital forensics, adding further to the debate and lack of distinctive nature of digital forensics as its own discipline. Few standards demonstrated how the topics, knowledge, skills and competences drawn were identified as relevant and effective for producing digital forensic practitioners.

Additionally, this thesis analyses and discusses results from 201 participants across five stakeholder groups: graduates, professionals, academics, students and the public. These areas were selected due to being underdeveloped in existing literature and the crucial role they play in the cycle of producing effective practitioners. Analysis on stakeholder views, experiences and thoughts surrounding education and training offer unique insight, theoretical underpinnings and original contributions not seen in existing literature. For example, challenges, costs and initial issues with introducing graduates to employment for the employers and/or supervising practitioners, the lack of awareness and contextualisation on behalf of students and graduates towards what knowledge and skills they have learned and acquired on a course and its practical application on-the-job which often lead to suggestions of a lack of fundamental knowledge and skills. This is evidenced throughout the thesis, but examples include graduates: for their reflections on education based on their new on-the-job experiences and practices; professionals: for their job experiences and requirements, academics: for their educational practices and challenges; students: their initial expectations and views; and, the public: for their general understanding. This research uniquely captures these perspectives, bolstering the development digital forensics as an academic discipline, along with the importance these diverse views play in the overall approach to delivering skilled practitioners.

While the main contribution to knowledge within this thesis is its narrative focusing on the education of effective digital forensic practitioners and its major stakeholders, this thesis also makes additional contributions both academically and professionally; including the discussion, analysis and reflection of:

- improvements for education and digital forensics topics for research and curriculum development;
- where course offerings can be improved for institutions offering digital forensic degree programmes;
- the need for further collaboration between industry and academia to provide students and graduates with greater understanding of the real-life role of a digital forensic practitioner and the expectations in employment;
- continuous and unique challenges within both academia and the industry which digital forensics possess and the need for improved facilities and tool development to curate and share problem and scenario-based learning studies.

ACKNOWLEDGEMENTS

I would like to pay special mention to the people who have been there to support me through this substantial work:

My supervisor, Dr. Paul Stephens, for providing me with this opportunity and for all his personal and academic support over the years. Without his continuous encouragement, patience, support and knowledge this thesis would never have reached completion.

My family for their ever-present affection, support and encouragement. In particular my mum, Gail, and dad, Sean, for being proud and standing by me no matter what throughout this experience.

My friend and colleague Joseph for his continuous encouragement, positivity and support at times in this journey when I thought all was lost.

My closest friends who have tolerated me throughout this journey throughout both the highs and lows and for time of proofreading.

My colleagues David, Ian, Abhaya and Gerald for the stimulating discussions and amusement we had in the last four years. I would also like to thank Prof. Robin Bryant, Dr. Steve Tong and Dr. Sabina Hulbert for their encouragement and advice.

Colleagues who I have worked with under the European Cybercrime Training and Education Group (E.C.T.E.G.); I thank you for the opportunities in development and delivery of digital forensics training for law enforcement.

My thesis committee for their insightful comments and encouragement, as well as their constructive feedback and questions.

Canterbury Christ Church University (CCCU) for providing me the opportunity to work within Computing, Digital Forensics and Cybersecurity, as well as funding for this PhD.

Finally, my sincere debt of gratitude goes to all participants who generously contributed to the work presented in this thesis. Without their insight, views and experiences, as well as time, this study would not have been possible.

ETHICAL CONSIDERATIONS

All contributing participants have been anonymised to protect their identities as well as their associated employers.

Participants were asked for their consent throughout this research study and were provided with the necessary information to make an informed decision of consent. For more information see Appendix H.

Contents

LIST OF TABLES

List of Figures

List of Abbreviations and Acronyms

Acronym – Meaning

ACPO – Association of Chief Police Officers.

BCS – British Computer Society.

BSI – The British Standards Institution.

CART – Computer Analysis and Response Team.

CATPCA – Categorical Principal Component Analysis.

CJA – Criminal Justice Act.

CMA – Computer Misuse Act.

CS – Computer Science.

CVF – Competency and Values Framework.

DFF – Digital Forensics Framework.

DFU – Digital Forensic Unit.

DLHE – Destination Leavers Surveys.

E.C.T.E.G. – European Cybercrime Training and Education Group.

FBI – Federal Bureau of Investigation.

FCG – Forensic Computing Group.

FSP – Forensic Service Provider.

FTK – Forensic Toolkit.

GCHQ – Government Communications Headquarters.

GDPR – General Data Protection Regulation.

GT – Grounded Theory.

GUI – Graphical User Interface.

HE – Higher Education.

HEI – Higher Education Institution.

HTCU – High Tech Crime Unit.

ICO – Information Commissioner’s Office.

ICT – Information Communication Technology.

IET – Institute for Engineering and Technology.

IISP – Institute of Information Security Professionals.

IOCE – International Organization on Computer Evidence.

IoE – Internet of Everything.

IoT – Internet of Things.

ISO – International Organization for Standardization.

ISP – Internet Service Provider.

IT – Information Technology.

KMO – Kaiser-Meyer-Olkin.

KSAs – Knowledge Skills and Abilities.

MBR – Master Boot Record.

NAT – Network Address Translation.

NCA – National Crime Agency.

NCSC – National Cyber Security Centre.

NIS – Network and Information Security.

NOS – National Occupational Standards.

NPCC – National Police Chiefs Council.

NSS – National Student Survey.

PACE – Police and Criminal Evidence Act.

PBF – Push Button Forensics.

PCA – Principal Component Analysis.

PGP – Pretty Good Privacy.

PII – Personally Identifiable Information.

PPF – Policing Professional Framework.

QAA – Quality Assurance Agency.

RIPA – Regulation of Investigatory Powers Act.

SSDL – Staged Self Directed Learning.

TEF – Teaching Excellence Framework.

TSK – The Sleuth Kit.

UCAS – Universities and Colleges Admissions Service.

USS – University Student Surveys.

LIST OF APPENDICES

1. INTRODUCTION

The rapid growth of small-scale digital devices and their integration into society has acted as a catalyst for aspects of people's home and work life where very few activities can be performed without leaving a digital footprint. Analysis of these devices, the data stored, and actions performed falls within the remit of digital forensics.

At its earliest inception, in the 1980s, digital forensics existed in industries such as law enforcement and was concerned with the analysis of singular devices such as a home computer or laptop used to facilitate a crime (Jones, 2004). Digital forensics has seen several challenges over the past decade, where difficulties have been encountered with technical capabilities, resources, and funding. More so, the rise in cloud-storage solutions, growth in storage sizes and emerging smart consumer technologies such as smartphones, watches, speakers and system essentials (e.g., appliances and security) are becoming more common in today's home and work environments and are a potential source for data within investigations.

The sheer number of devices which may be seized in an investigation, along with large volumes of storage available in devices have left forensic analysts with workloads too high to manage causing lengthy backlogs in digital forensic units (DFUs) (Mislan, Casey and Kessler, 2010; Gomez, 2012; Lillis, O'Sullivan and Scanlon, 2016; Montasari and Hill, 2019). Furthermore, these challenges have led to forensic analysts becoming what some have noted as 'button pushers' where fewer investigations may be conducted using knowledge, skills and abilities of the practitioner and reliance is heavily placed on the functionality of standard industry tools (James and Gladyshev, 2013b). Here lies the question of what makes an effective practitioner: is it an analyst who can use an automated tool to process and analyse device contents, or is it a person with the underlying knowledge, skills and abilities to also be able to perform these tasks manually to corroborate tool findings?

While the mass of information and devices has become overwhelming for investigators, further challenges identified have included encryption, virtual networks, cloud-data forensics, live forensics through to legal challenges (Fahdi, Clarke and Furnell, 2013; McMillan, Glisson and Bromby, 2013; Spiekermann *et al.*, 2017). Furthermore, people's awareness of the immense amount of data stored on their devices and careless attitudes towards securing their data and protecting themselves from harm online has also become a worrying factor. Problems such as data loss, data security, and a rise in criminal activities reliant on technology and Internet-connected devices has been seen; yet with technology set to continually develop and become more intelligent these woes may be heightened further. High profile incidents such as, Yahoo!, Sony's PlayStation Network and Facebook and Cambridge Analytica which saw huge data breaches with companies fined for failing to keep personal information secure; highlighting the dangers and damages which can be caused with people's data (Leyden, 2013; Information Commissioner's Office, 2018e; Information Commissioner's Office (ICO), 2018). Since then several concerns have been voiced over system securities as well as accessibility and use of personal information stored on these devices. It has also been reported in the UK Cyber Security Strategy published by the Cabinet Office (2016, p. 22) that awareness surrounding "poor cyber hygiene and compliance" has increased in the last few years.

While awareness has increased there are still a range of vulnerabilities towards security mechanisms and precautions among the general populous. Much research has highlighted a lack of information security awareness and technical skills where humans are attributed as the weakest link intentionally or unintentionally in the process of information and cyber security (Solms and Niekerk, 2013; Dunn Cavelty, 2014; Kortjan and Solms, 2014; Parsons *et al.*, 2017; Aldawood and Skinner, 2018). While security of digital devices and data are concerns to ensure limited damages in digital and cyber-related attacks, the data stored on a variety of apparatuses and online services are and have potential to become even greater assets for digital investigators in corporate, civil and criminal investigations.

While the digital forensic discipline has existed for over three decades in industry, it arose in the early-mid 2000s in an educational context (Yasinsac *et al.*, 2003; Leyden, 2005). Traditionally, analysts and technicians were educated through on-the-job training until the delivery of educational and training programs which are now used to acquire knowledge, skills and abilities in several topic areas within digital forensics. Documented as an interdisciplinary subject, the subject has yet to find its footing as a clear academic discipline. Often incorporated into departments of computing, engineering, mathematics, criminology and policing its interdisciplinary nature and strategies to achieve cyber secure nations may have played in most recent shifts to cyber security within higher educational provisions and, by extension, digital forensics.

Literature often concentrates on learning styles and delivers attempts to outline course structures to define the academic subject (Irons, Stephens and Ferguson, 2009; Thomas, Tryfonas and Sutherland, 2009; Irons and Thomas, 2014; Karie and Venter, 2014; Miranda Lopez, Moon and Park, 2016; Kiper, 2017); however, the discipline is missing research which looks at the effectiveness of course content and the production of effective professionals, including graduates for industry. The clarity of topics and course content covered is widely unknown for digital forensics as discussed by Thomas, Tryfonas and Sutherland (2009). This makes it challenging for stakeholders, including professionals and potential students alike, to identify what knowledge, skills and abilities will be gained. There is little research that analyses courses provided within higher education in the UK that illuminates structure and importance of topics within such courses.

Furthermore, considerable scholarly research has been conducted into areas of digital forensics such as traditional computer forensics and investigative procedures. While digital forensic investigations somewhat follow an ontology and harness fundamental principles, practices and procedures, the discipline has suffered from debates and challenges over standardisation and certification for several years (Grobler, 2010, 2012; Karie and Venter, 2014). More recent debates have seen the discipline question standardisation during development, and implementation, of the Forensic Science Regulator's efforts to validate digital forensics laboratories and tools to show standardisation within industry and deliver compliance using ISO 17025 (The Forensic Science Regulator, 2016; International Organization for Standardization (ISO), 2017). Similarly, educational developments have suffered from a lack of standard procedures and certification processes to ensure clarity among course offerings in digital forensics.

Recent efforts have seen the development and delivery of guidelines for cyber security curricula and, by extension digital forensics; still, these raise more questions when seeking to define digital forensics as a distinct academic discipline. The literature lacks review of these guidelines and certifications; for example, towards their development, applicability, implementation, benefits, and academic costs have yet to be determined. While such works show promise in standardisation within digital forensics and cyber security, arguably they may also demonstrate several flaws and potential for bias.

With questions around the clarity of course outlines or content and issues with standardisation, there is no identification of 'effectiveness' of courses within the UK higher education system, or what constitutes an effective practitioner. Similarly there poses the question of who should determine what makes an effective course and effective practitioners, as this will be essentially subjective to people's own experiences. This study promotes this should be a collective and collaborative effort among a range of stakeholders involved within the field of digital forensics and education to identify the fundamental knowledge, skills, and abilities intrinsic to all sectors involving digital forensics in order to be deemed 'effective'. Largely, a degree programme's effectiveness is measured by student surveys and employability statistics such as the UK Engagement Survey (UKES) and the Graduates Outcomes survey (Higher Education Academy, 2019; Higher Education Statistics Agency (HESA), 2019). These can be used to identify student satisfaction of a course and leavers' employability. Though these statistics do not elucidate how effective each course or curricula are for the graduates or employers. For example, they do not provide an understanding of the positives and negatives of graduates for industry, the skills, and competences they acquire and take into industry, or the topics which have been delivered on a course.

Measuring the effectiveness of a course is complex and several training courses within digital forensics have shown use of Kirkpatrick's training evaluation model to accomplish evaluation (Stephens, 2012; Genoe, Toolan and McGourty, 2014). The model uses four levels (reaction, learning, behaviour, and result) (Kirkpatrick and Kirkpatrick, 2006) to evaluate overall enjoyment, usefulness, knowledge acquisition, performance, and results for the wider community. Yet few works have considered overall effectiveness of higher education courses within the discipline based on these factors of evaluation nor stakeholder opinions or experiences. Effectiveness may be considered, for example, by reflecting on course coverage, content, outcomes and graduate competences and their suitability within a fast paced and continually changing discipline and industry.

While there is some research into the digital forensic curriculum and training, there is little by way of narrative, i.e., drawing on experiences and views of a variety of stakeholders linked with the academic discipline to understand what is required and what is effective. Research for digital forensics education has often focused on specific technical teachings, course development and delivery as well as learning and assessment. Yet there is no cohesive study which concentrates on the views, ideals, experiences and expectations of the people who play a role within the discipline and those who are reliant on education and training.

The basis of the problem statement for this research is the lack of narrative (i.e. descriptive accounts and experiences) from stakeholders within industry and academia alike which draw on the expectations of a digital forensic practitioner. Particularly in an era where more focus is being placed on cyber security as seen in the shift within higher education. This research looks to identify courses which offer digital forensics in the UK, analyse commonalities among topical content and discuss challenges within the academic discipline of digital forensics. While courses should be flexible and content coverage diverse, this study looks further at recent frameworks for digital forensics and their attempts to help define, shape and identify quality and expectations within a niche discipline and towards delivery of effective digital forensic practitioners. Furthermore, this research looks to draw together these efforts with the views of stakeholders within digital education including: professionals for their experience and position as an employer; academics who educate the upcoming workforce; graduates and students for they are key players in the evaluation process; and, the public for their opinions of both digital forensics and cyber security as disciplines. Despite there being no precise approaches to measuring the effectiveness within digital forensics, this thesis concentrates on synthesising stakeholder accounts to deliver an understanding whether education and training are producing knowledgeable practitioners and examine how education and training for digital forensics can be improved.

1.1 Research Questions

This section highlights the research questions which are interwoven throughout this research. Each question is accompanied by several sub-questions in order to address them in a better light.

Q1: What is the current curriculum for digital forensics?

This question involves an understanding of the placement and diversity of research previously conducted within academia, in professional contexts and of the identification of courses at undergraduate level throughout the UK. A literature review forms the basis of this research question. This question prompts several sub-questions to define the relevancy of the literature and course outlines in the development of course curricula within digital forensics and cyber security. For example, what topics are included within a digital forensic degree? what makes one course stand out from the other? what makes the course a digital forensic degree and not computing or computer science? and, what is the meaning of accreditation within the discipline? Sub-questions also range and relate to the educational and training delivery methods, and further the understanding towards a development tool facilitative of the production of effective practitioners. For example, how important is experience and training versus education within the discipline? and, how can a tool for scenario creation facilitate better teaching and learning in education and training? This question and its sub-questions greatly assist in answering the overarching question of this study of *what makes an effective digital forensics practitioner?*

Q2: What developments can be made towards a curriculum framework reflective of industry needs?

This research question aims to identify and discuss the delivery of curriculum frameworks within digital forensics, for which there are none in existence at the start of this study. Throughout this research provisions for digital forensics through cyber security frameworks and certifications have been implemented. This question seeks to understand the complexity of developing, delivering and implementing such frameworks in a distinct and fast-moving discipline, while also seeking to understand the implementation of frameworks within the disciplines.

Q3: What makes an effective digital forensic practitioner and/or curriculum?

This question encapsulates the central and underlying themes of this research, pursuing the identification of the impact of educational and training programs on the production of effective practitioners within digital forensics. In many practical and specialist subjects, on-the-job learning can be more valuable than education in a lecture theatre - take medical professions for example. Considering this, the research aims to explore the curriculum in digital forensics to identify if target audiences find higher educational programs to be fruitful and effective in the development of professionals or whether more experience-based programs would be influential for career growth. The main aim is to further understand how practitioners put into practice what they have learned in education and training programs and what could improve the process. The question converges on the foundations of what people feel are 'important' and 'effective'. This leads to several accompanying questions, for example: do educational programs deliver effective graduates for digital forensics professions; do learning methods in the curriculum support the industry needs; do students and graduates value their education and learning; are training courses relevant, and central to digital forensics development. To understand this, views and experiences from five stakeholder groups are obtained to provide narrative and give voice to the very people who are part of the digital forensic discipline.

1.2 Research Aims and Objectives

Firstly, it is important to consider the field of digital forensics is fast paced and continuously developing. As a result, some of this thesis might discuss issues which have now been partly or fully addressed (for example the delivery of framework standards in cyber security and subsequently digital forensics education; though the question which may be asked is: are they reflective of industry needs?).

The vision of this research is to provide an understanding of the current situation for digital forensics education, how the profession is progressing, in addition to what knowledge, skills and abilities are most expected of a graduate with a digital forensics related degree. This research looks to achieve these aims by understanding the current position of digital forensics in a cyber security led field, identifying challenges within higher education. Questionnaires and interviews are used to collect views and experiences of digital forensic practitioners in order to discuss requirements of the curricula. While also enabling and determining what is essential for a practitioner in the field and what makes them effective. Existing literature will be used throughout, alongside first-hand accounts of a range of participants. Focus will be centred on identifying the views of the very people who support and are an essential aspect within the discipline.

The underlying assumptions of this study are that those working and studying within higher education are likely to have differing views compared to those who have completed their studies or are working in industry. This difference is likely due to their diverse experiences. Experiential influences might be based on a respondent's length of service in the profession, through to encounters with training or teaching programs. Further assumptions are based on the researcher's experiences and the research questions posed.

The Aim: to assess digital forensics education in the UK and consider what factors facilitate/constitute an effective practitioner.

The Objectives

- To describe and assess the current state of digital forensics in the UK higher education system and determine its potential progression.
- To identify the main factors and challenges impacting the development and delivery of digital forensics education.
- To assess perceptions, views, and experiences of several stakeholders within the discipline of digital forensics and determine similarities and differences to pinpoint current challenges with educating individuals considered for roles within the digital forensic industry and their efficacy.
- To propose recommendations to curriculum developers and industry stakeholders in terms of increasing the level of effectiveness of education and alumni for employment.

1.3 Research Contribution

This research builds on the work of others within the field of curriculum research for digital forensics. Original contribution, emerging from gaps within the saturated research of computing, is applied using qualitative approaches discussing and exploring the effectiveness of education and training within the discipline and the essentials for producing effective practitioners.

Table 1.1 demonstrates potential beneficiaries of this research and perceived benefits in the view of the researcher. Following potential beneficiaries, this section outlines the contributions this research makes to digital forensic literature.

Potential Beneficiaries	Example Benefits
Academics/Trainers	- Literature survey of the current state of digital forensics curriculum - Identification of key topics for research and areas for curriculum focus/development - Review of existing framework associated with digital forensics and cyber security
Practitioners	- Experiences and views of multiple target groups - A broader understanding of current state of digital forensics curriculum in higher education
Students Potential Students Guardians	- Understanding of requirements and challenges in the delivery of higher education programmes for digital forensics - Experiences and views of multiple target audiences (e.g. what professionals look for; what education provides them; what skills they need to develop and apply)
Public	- Potential identification of areas of understanding and knowledge to be spread and learned

Table 1.1 – Potential Beneficiaries of this Research

This research will contribute to knowledge in the following ways;

- provide data on:
    - the view of academics who design and deliver courses in digital forensics and cyber security;
    - what professionals expect of a digital forensics' practitioner and their experiences in/of education and training;
    - alumni feelings and expectations of education and in their roles gained;
    - the view of some very early students studying digital forensics and cyber security courses on the discipline(s), education, and industry;
    - the view of some public participants on the view of digital crimes, digital forensics and cyber security, plus the education of the public;
- provide a review and analysis of:
    - curriculum frameworks within the discipline, with discussions over future development based on the research contributions;
    - stakeholder responses to consider curriculum design/challenges and industry challenges;
- interpret the data to discuss ideas and challenges based on people's views within and across stakeholder groups, as well as their opinions, knowledge, experiences, or values;
- suggestions toward future improvement in the curriculum design of digital forensics.

Originality of this research has delivered several peer-reviewed articles and academic workshops, demonstrated in Appendix G, where some of these published works have been included within this thesis.

1.4 Organisation of the Thesis

Chapter 1 introduces the research focusing on the current gaps within the literature, stating the problem and research aims and objectives.

Chapter 2 discusses the literature surrounding the development and delivery of digital forensics in higher education in effort to identify current offerings and challenges with undergraduate degrees within the UK HE system. Literature examined also focuses on learning and teaching methods currently utilised within digital forensics education to provide the reader with an understanding of implementation and practice within educational offerings. Further, this thesis identifies where a largely practical educational discipline can learn from other practices and their delivery in higher education. This chapter also provides a review/analysis of several courses across the UK, breaking down the content provided based on publicly available information in such a manner that an overview of what the student curriculum looks like in digital forensics through description and analysis.

Chapter 3 discusses the current literature available which focuses on existing knowledge of digital forensics and cyber security as respective disciplines and the challenges surrounding defining these as disciplines, in particular, digital forensics and its placement as an academic discipline. This chapter goes on to look at the newly devised frameworks which look to certify and standardise educational practices in largely cyber security and digital forensics, reviewing works so far to provide the reader with an understanding of existing models and challenges.

Chapter 4 explains the chosen research methodology in four stages. Firstly, this chapter highlights the research questions and aims. Secondly, this chapter deals with the context and strategy of the research and the 'why' and 'how' a qualitative research approach is adopted, espousing a much broader discussion. The third section of this chapter focuses on the design of the research methodology, concentrating on the methods used throughout to capture responses and analyse the data. While the fourth section places attention on the interests, and the background, of the researcher identifying how the researcher's own experiences may in fact help shape the research ideas and analysis. Overall, this chapter explains the implementation of methods/instruments used throughout this research, along with discussion and justification.

Chapter 5 reports initial results from a small-scale study seeking information regarding 'resourcing a digital forensics programme in higher education'. This chapter explores issues such as specialist equipment, costs associated with tools, accreditation and observations on behalf of academics. While also looking at the challenges which educators face considering learning and teaching methods which require practical evidence.

Chapter 6 focuses on the views, beliefs, experiences, and overall responses from three groups of stakeholders considered in this study: academics, graduates and students. This chapter analyses topics or subjects which stakeholders believe are necessary for skilled practitioners and are a requirement for the delivery of digital forensics education. Furthermore, skills and attitudes are discussed among the need to balance stakeholder interests and opinions.

Chapter 7 focuses on the views, beliefs, experiences, and overall responses from professionals as stakeholders looking at expectations of graduates and practitioners alike. Analysing key topics and skills for the assessment of the delivery of digital forensics education and to provide a narrative to a key stakeholder group within the discipline.

Chapter 8 captures a range of views from participants from the wider public audience. Outcomes focus on identifying the people's opinions and views adding insight into what is understood of digital forensics and/or cyber security by a wider audience than the stakeholders questioned in previous chapters. Public participants are included to determine wide-ranging views on issues in relation to digital crimes and what should be tackled in society as well as by law enforcement officials. Interests were also placed on finding out views of individuals who have fallen victim of such crimes, the crimes committed and their response to these situations to identify awareness among individuals.

Chapter 9 discusses the overall results of stakeholder views for what makes an ideal course while cross examining the idea of an effective digital forensics practitioner from the narrative views, experiences, expectations, and requirements described. This chapter also discusses the implementation of a set of roadmaps that form the main contribution in chapter 10 and may be used by various stakeholders to ensure that the digital forensic curriculum is as effective as possible based on several factors built up from the narratives, views and experiences considered in this chapter.

Chapter 10 concludes this study, noting further work that is required to continue to keep abreast with technological and educational changes and challenges in effort to develop the discipline further.

2. A Review of Digital Forensics in Higher Education

Introduction

This chapter focuses on available literature surrounding the development and delivery of digital forensics in higher education in the UK. In order to understand the current position and challenges of the discipline a review of this field within higher education, training and professionally from its earliest appearances is essential. This review concentrates on course growth, delivery and training of digital forensics within higher education, featuring challenges faced with, for example, learning and curriculum development and application of the discipline. The literature highlights there is a need for greater understanding of what makes an effective digital forensic practitioner from multiple stakeholders, i.e., those who are involved in roles within the discipline, including; academia and industry.

2.1 Digital Forensics versus Cyber Security

The divergence on the meaning of digital forensics and cyber security as disciplines are an ever more growing debate. With university degree programmes having moved toward the inclusion and attention on cyber security, the definition and position of both exist with many similarities yet, substantial differences. Current naming conventions for degree programmes include keywords such as ‘cyber’, ‘security’, ‘digital’, ‘forensics’, ‘computer’ and ‘networking’ with an amalgamation of terms and meanings. The positioning of both disciplines is often still questionable and less distinct.

Schatz, Bashroush and Wall (2017) discuss how terminology such as Computer Security and IT Security were used originally with professionals understanding the known differences of the two, however, they discuss that for wider audiences such similarities can reduce the clarity among terminology used. The authors (Schatz, Bashroush and Wall, 2017) particularly emphasise this in relation to cyber security where they also argue the need for a more representative view of the discipline due to what they “recogni[se as a] lack of a consistent meaning of the term cyber security”.

For many cyber security is recognised as “a subset of the broader discipline of *information security*” (Kessler and Ramsay, 2014, p. 4932) and across many forms of research, naming conventions for education and training, and further afield are used interchangeably. What is interesting at this stage is the key difference between cyber security and information security. Cyber security is all about the digital realm (i.e., the protection of information from vulnerabilities of networks and systems) (International Organization for Standardization (ISO), 2012). Whereas information security concerns itself with the security of any type of information regardless of the realm (e.g., the appropriate safe housing of information in an organisation stored and accessed in several ways, be it digital or paper records) (International Organization for Standardization (ISO), 2018).

The same has been discussed of digital forensics where Vincze (2016) acknowledges a range of terms used such as computer crime, cybercrime, digital/electronic crime and so on. Vincze (2016) continues to note that cybercrime by those with a professional understanding of the disciplines brings a different set of challenges than the original examination of digital and electronic devices. Thus, initiating the same discussion for a familiar and consistent meaning of both digital forensic and cyber security, not just among professionals. Arguably, the largest similarity of the two disciplines is the need for both in the current digital age; where, we see continuous developing technologies, increased provisions around privacy, security and consent and a heavy reliance on the Internet and smarter devices.

Typically, computer or digital forensics was often recognised as a requirement of policing and governmental work. However, over the years the requirements for such skilled practitioners in digital forensic positions has been established across a range of medium and large corporations (e.g. insurance, banking and so on). Cyber security in businesses has also seen “substantial investment … [f]ollowing the real-world impact of some high-profile breaches … [where,] businesses are also placing much greater emphasis on resilience, recovery and response to breaches.” (Institute of Chartered Accountants in England and Wales, 2018, para. 2).

The two disciplines are also intertwined by their common need for the inclusion of digital devices, assets, data and intelligence. Businesses began to identify the need for professionals in securing systems, technologies and assets while also the need for professionals who could gather data and potential evidence on crimes committed (both external and internal). Storage and security of customer data is paramount and, to some degree, more in the hands of the customer as of 2018 than ever before due to the General Data Protection Regulation (Council of Europe, 2016); these skills are vital to sound and secure working practices.

Over ten years ago, Kanellis, Kiountouzis and Kolokotronis (2006, p. 250) highlighted overlaps the discipline of digital forensics had with information technology governance and information security. Still to this day digital forensics has common ground and interlinks with these close subjects (as discussed in chapter 2). The same can be said for cyber security, where authors highlight interdisciplinary workings of the discipline focusing on areas such as, computing, information security, business and management, law and governance to name a few (Omar, Venkatesan and Amamra, 2018, p. 5). Ramirez (2017, p. 3) argues that cyber security "comprises [of] four different subdisciplines: policy, computer science, management, and social science", citing a range of topics covered by each of the four areas including topics such as, national security, ethics, cryptography, computer and operating systems and behavioural science (Ramirez, 2017, p. 30).

Some describe the two disciplines (digital forensics and cyber security) "as two essential sides of the same coin" (Krakoff, no date). Though broadly digital forensics has been described as a branch of forensic science, people may view the discipline as a subset of cyber security. This is often seen within many cyber security frameworks (Joint Task Force on Cybersecurity Education, 2017; NCSC, 2017b; Newhouse *et al.*, 2017) and more often seen in the delivery of cyber security courses in HE (emphasised in chapter 4).

Though the two disciplines are not one and the same, they are dependent upon one another for successes in their goals to preventing or investigating a crime. Therefore, a similarity of the two, is the essential ingredient to "increase coordination between [the disciplines] … to best track and convict cyber criminals" (Dlamini, Eloff and Eloff, 2009, p. 196). For example, in a blog post by Gregal (2014), they state that "[i]n almost all security breaches, a crime has also been committed, and at this point, security and forensics join together to become one crime fighting team." Gregal (2014) continues to discuss how forensic practitioners rely on security teams for not only securing systems (e.g., patching vulnerabilities, permissions, and other controls) but for accurate and complete logs which can facilitate in identifying the crime, threat and perpetrator, all of which can help a forensic investigation.

In the same way that there are similarities of information security and cyber security, the two disciplines of digital forensics and cyber security hold some similarities in their usage, skills required, and career prospects. Moreover, although the two disciplines work in tandem, they do deliver differences which can be used as a distinction when used interchangeably to many outsiders of each field.

Throughout this thesis the terms digital forensics and cyber security are written separately to highlight the two as distinct disciplines. The largest difference between the two being: security is the approach taken before a crime as a form of resilience and protection of information in the cyber realm; a proactive approach. Digital forensics, on the other hand, is an examination of data/information on digital devices after criminal activities have occurred; a reactive approach.

	Digital Forensics	**Cyber Security**
Similarities[1]	Interdisciplinary nature: computer science, information security, engineering, mathematics, forensics, law and criminal justice, criminology, policing, business and management (Irons, Stephens and Ferguson, 2009; Ramirez, 2017)	
	Fundamental knowledge of digital infrastructure: computer systems, operating systems, networks, risk assessment and management, software engineering/computer programming (Joint Task Force on Cybersecurity Education, 2017; NCSC, 2017b; Newhouse *et al.*, 2017)	
	Governance: policies procedures and principles, legislation and standards) albeit different approaches and policies followed – a strong link with accountability (Grobler and Louwrens, 2006; Grobler and Dlamini, 2010)	
	Preservation: the idea of safeguarding, be it protecting a system from threats or preserving evidence for an investigation	
	Behavioural analysis: the ability to think like a criminal and to understand how/why/what a criminal thinks and acts like (Shinder and Cross, 2008, p. 81; Vidalis, Llewellyn and Angelopoulou, 2010)	
	Competence: the technical knowhow to handle duties, data and evidence (potentially outside the remit of known practices)	
	Skills: problem-solving, critical thinking, initiative, self-direction, creativity, management, accuracy, organisation, people skills and so on	
Differences[1]	It is the collection, preservation, acquisition and analysis of digital devices to understand a crime (Reith, Carr and Gunsch, 2002a, p. 2)	It is the process of protecting and defending information systems from threats in cyberspace (Luiijf, Besseling and De Graaf, 2013)
	DF practitioners are told of a system breach or criminal activity and asked to investigate using devices, data and records	CS practitioners identify the system breach or potential crime and alert forensic examiners or incident responders
	Investigates if a crime has taken place and potentially who committed it; reactive (Alharbi, Weber-Jahnke and Traore, 2011, p. 67)	Takes place before a crime is committed or after in order to improve security; requirement to be more proactive (Rowe and Gallaher, 2006)

Table 2.1 – Similarities and differences of two interchangeable disciplines (digital forensics and cyber security)

For completeness and clarity, the term ‘Forensic Readiness’ should also be addressed in the debate of digital forensics versus cyber security. In its simplest form, forensic readiness is an organisations ability to respond to the collection, preservation, and analysis of digital evidence related to an incident, while demonstrating due diligence. The (CESG Good Practice Guide (2009) cited in Digital Continuity to Support Forensic Readiness, 2011, p. 8) defines forensic readiness as:

> “The achievement of an appropriate level of capability by an organisation in order for it to be able to collect, preserve, protect and analyse Digital Evidence so that

[1] In their simplest form.

> this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or in a court of law."

ISO 30121 (International Organization for Standardization, 2015) defines forensic readiness in a similar form and states that it

> "assures that an organization has made the appropriate and relevant strategic preparation for accepting potential events of an evidential nature … In every situation, IT should be strategically deployed to maximise the effectiveness of evidential availability, accessibility, and cost efficiency."

Furthermore, ISO 27043 (International Organization for Standardization, 2015b) notes that the forensic readiness process is part of a digital investigation. Where a digital investigation is defined as:

> "use of scientifically derived and proven methods towards the identification, collection, transportation, storage, analysis, interpretation, presentation, distribution, return, and/or destruction of digital evidence derived from digital sources, while obtaining proper authorizations for all activities, properly documenting all activities, interacting with the physical investigation, preserving digital evidence, and maintaining the chain of custody, for the purpose of facilitating or furthering the reconstruction of events found to be incidents requiring a digital investigation, whether of criminal nature or not."

Thus, digital forensic readiness focusses on the ability to conduct digital forensic investigations through all phases of an investigation. While proactively planning, managing, and organising activities, scenarios, and sources of evidence, acknowledging capabilities and requirements, minimising costs, assessing risks, ensuring sufficient records are kept for subsequent forensic related tasks, conducting systematic and cost-effective investigations, and considers continuity and authenticity as fundamental pillars.

2.2 The Rise of Digital Forensics and Higher Education Pathways

Technology as we see it today is ubiquitous, emergent, and advancing at a tremendous rate. With 24/7 access to high-tech tools and environments there has been a rise in digital and digitally enhanced crime if only for the heightened awareness of attacks on high profile companies. Digital forensics is undoubtedly a domain which has grown with and towards the rising trends of these digital technologies alongside the necessity to combat digital crimes. Digital forensics today plays a role in most, if not all, investigations into unlawful acts where the need for skilled practitioners to examine and investigate areas of digital, cyber and security related crimes has led to the development of higher education pathways and professional on-the-job training courses aimed at delivering skilled individuals with more than previously accepted IT backgrounds.

With all these elements, investigations, in comparison to the 1990s and 2000s, are conducted on a much larger scale. It is not solely the magnitude of digital crime which has increased, but the number of technological devices at the tip of our fingers. This cultural shift continues to rise, and further the volume of data which we can, and do, store. These technological advancements have in turn, over the years, increased the number of devices seized and those requiring examination. These digital storage devices, the bits and bytes of data to be sifted through, impose a knock on effect, creating lengthy backlogs, particularly within the public sector industry (Parsonage, 2009; Gomez, 2012).

In today's economy where, digital crime is far beyond the demands of the past few decades, specific skills are sought after for such a practitioner. It can also be said that over time there has been an increased chronic skills shortage in the area. Nowadays, much of an investigation is undertaken using Graphical User Interface (GUI) driven tools, or otherwise known as "push-button forensics (PBF)" tools with practitioners heading towards less reflectivity (James and Gladyshev, 2013b, p. 1).

Computer forensics education embraces a breadth and depth of knowledge and can be described as multi/interdisciplinary. At minimum the subject consists of the triangulation between Computer Science, Forensic Science and Criminology (Figure 2.1) and intrinsic qualities adopt both theory and technical practice. Due to these qualities, approaches and skills the discipline also contributes to the very subjects it draws from where these continue to strengthen the "rigour and robustness" for its own standing as a single discipline (Irons, Stephens and Ferguson, 2009, p. 84).

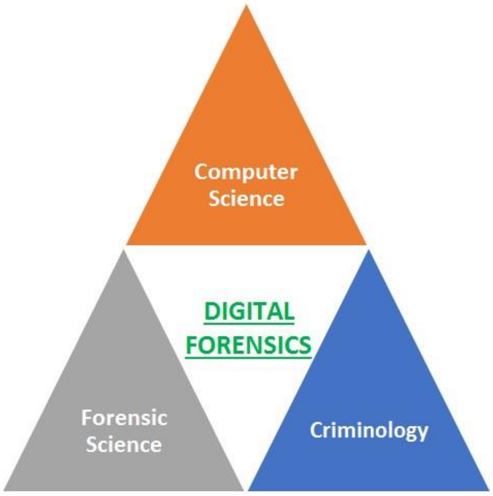


Figure 2.1 – Triangulation of Digital Forensics

Over the past decade the development of programmes, both undergraduate and postgraduate which offer digital forensic content has matured, particularly in countries such as the United Kingdom, Ireland, the United States and Australia (Yasinsac *et al.*, 2003; Kessler and Schirling, 2006; Liu, 2016).

Universities UK (2015) has shown there to be a decrease in student enrolments within computing where, other STEM subjects such as engineering and mathematics have seen an increase in numbers in the past ten years (Higher Education Statistics Agency (HESA), 2017). While computing related courses have witnessed a decline, there has been a rise in the number of courses on offer which capture an essence of digital forensics. In 2005, there were just five 'Computer Forensics' courses in the UK (Leyden, 2005). Courses then were generally named 'Computer Forensics', due to their nature of managing evidence relating only to computers. Many of these courses at that time were of master's level before development of undergraduate programmes. With advances in technology, and a greater emphasis on a mobile-centric nation, the discipline has grown to be known as 'Digital Forensics'. The swap from 'Computer' to 'Digital' Forensics is used to describe the subjects' current paradigm of managing expansive quantities of data and multiple digital devices.

Thomas, Tryfonas and Sutherland (2009) conducted a study looking at and analysing the components of a computer forensics degree where they observed "course title is very important for marketing purposes and an interesting, eye catching course title was vital to the success of a course", where 'Computer Security & Forensics' and 'Digital Forensics' topped the chart preferences of nineteen delegates. Courses have since continued to be reviewed and ripened, enriching the market with numerous course titles e.g., 'Forensic Computing', 'Computer Forensics and Security', 'Computer and Digital Forensics' and 'Digital Security, Forensics and Ethical Hacking' (Universities and Colleges Admissions Service (UCAS), 2015). In 2017 many of these naming conventions still existed (as depicted in Table 2.2).

Course Name	Count	Course Name	Count
Computer Forensics	5	Computer Science & Forensics Science	1
Computer Forensics & Security	3	Computer & Information Security	1
Computer Forensic Investigation	1	Computer & Digital Forensics	2
Forensic Computing	4	Computer & Cyber Forensics	1
Forensic Computing & Security	2	Computer Systems (Forensics & Security)	1
Computer Security	1	Computing (Network and Forensics)	1
Computer Security & Forensics	2	Computing (Networking, Security and Forensics)	1
Computer Security with Forensics	1	Applied Computing (Cyber Security) Top-up	1
Digital Forensics & Cyber Security	1	Cyber & Computer Security	1
Computer Science with Cyber Security	1	Cyber Security & Computer Forensics with Business	1
Computer Science & Criminology	1	Policing Studies & Computer Forensics	1

Table 2.2 – Popular Digital Forensics Course Titles in 2017 based on UCAS Search (UCAS, 2017b)

However, as Thomas, Tryfonas and Sutherland (2009) further discuss the variety of course title does not depict the content of a module or entire programme let alone determine the effectiveness of a course curriculum by its attractiveness.

Through comparison of previously gathered course briefings, collated in 2014 and those gathered today, it is observed that at least eight HEIs have amended their course names, or made additions or subtractions to courses available. In more recent years course offerings have shifted to include cyber security, this may be due to increased funding and alarming rates of skills shortages identified within the security sector in order to produce workforces equipped to combat cyber-attacks (Cabinet Office, 2016). Furthermore, authors have highlighted how national strategies for several years have mentioned "strengthening of their digital police and digital forensics capabilities" as analysed by Luiijf, Besseling and De Graaf (2013). Cybercrime has been heightened in part due to its "tempting" nature, convenience, and technological advancements (Hargreaves and Prince, 2013; Chawki *et al.*, 2015). However, across programmes the 'cyberness', is still new and, is something which will no doubt continue to infuse into digital forensic programmes as well as forensic science, policing, law and criminology. Alva and Endicott-Popovsky (2012, p. 75) discuss how "[t]here is an alarming gap in the legal and judicial community's understanding of digital evidence" and again where authors discuss the need for awareness of digital forensics "experts" in court settings (Henseler and Loenhout, 2018). Bagby and Ruhnka (2006, p. 57) point out how courses must highlight "interdisciplinary challenge[s] in professional Cyberforensics practice because skills learned by this technique must be accurately applied to technical processes".

Figures and literature have also shown that in the last decade, there has been greater uptake on developing courses in the area of digital forensics and cyber security. UCAS (Universities and Colleges Admissions Service (UCAS), 2017) records, at the time of writing, show more than thirty undergraduate programmes relating to digital forensics, particularly at post-92 universities. Based on datasets accessed from UCAS EXACT, a UCAS Media Service, and data from Higher Education Standards Agency (HESA) the number of student acceptances[2] has for many years averaged near to the 20s during the time period 2011-2016 for courses containing the name 'forensic' (e.g., computer forensics, digital forensics, security and forensics). Mindful of the restrictions around data disclosure and implemented rounding methodologies (e.g. rounding and suppression to the nearest multiple of 5 (HESA, no date)) which were applied to reduce the risk of disclosing personal data, figures show that the average for 2011 stood at approximately 15 people. The highest number of acceptances for one institution was recorded as 80 people (rounded). The same approach was adopted for data from 2016, where an average for accepted applicants was rounded to 20 people. The

[2] Acceptances are defined as "an applicant who has been placed for entry into higher education" including prior acceptances recorded previously (UCAS, 2017a).

highest number of acceptances for one institution reached 95 people (rounded) across two course codes. Each time this was the same institution reaching a higher than average intake of accepted students.

When looking closely at the rounded data for 2016 the highest number of applications recorded for a course involving an element of digital forensics was 290, however, only 35 students were recorded as being accepted. For the same institution back in 2011, their rounded application numbers stood at 175 with an acceptance of 25 students. A similar trend which can be found across most institutions offering digital forensics and cyber security courses where there are smaller numbers of students accepted on to the degree programmes. In 2011 and 2016 the most popular rounded value of acceptances among the courses containing ‘forensic’ were between 5 and 35 students. These figures, however, do not account for retention of student numbers across the three years of study.

HESA data figures between academic years 2010/11 through to 2015/16 show that the number of students in their first year of instance in each reporting period across undergraduate and postgraduate courses relating course keywords[3] increased in later years. The period 2015/16 saw the highest record of first year students recorded at 2035, accounting for approximately 20 percent of the total reported in their first-year instance within that time period. However, this figure only accounts for approximately eight percent of the total students recorded as studying such a course across UK HE, including those not identified as being in their first-year studies. Figure 2.2 highlights the number of students identified in their first year of study as well as those not identified in their first-year instance in each reporting period between 2010 and 2016.

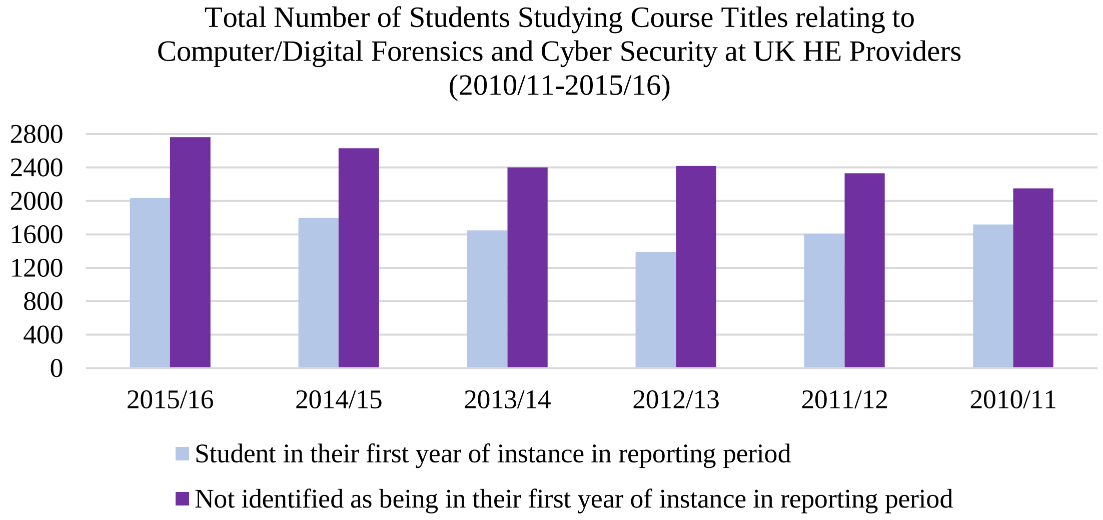


Figure 2.2 – Total Number of Students Studying forensic/security courses from HESA dataset (2017)

[3] Keywords: ‘comput’ and ‘forensic’, ‘digital’ and ‘forensic’, ‘comput’ and ‘security’, ‘cyber’ and ‘security’

The figures show that in the last decade the number of students has risen year-on-year except for the reporting periods 2011/12 and 2012/13 where numbers in their first year of instance showed a slight fall. This reduction is harmonious with the trend in fewer applicants and acceptances across the UK HE system at this time attributed to the rise in tuition fees which nearly trebled for students in 2012. UCAS (2012, p. 5) reported that "[t]here were 51,000 (-13 per cent) fewer acceptances into English institutions in the 2012-13 academic year than in the previous year".

2.3 The Current State of Digital Forensics Education in UK Higher Education

Within the academic community research has been conducted on programme design and learning techniques, where progression is seen through a number of course outlines and experimental ways of delivery and learning (Anderson *et al.*, 2006; Kessler and Schirling, 2006; Irons, Stephens and Ferguson, 2009). It has been recognised that programmes should deliver both technical/practical and theoretical attributes within computing, digital forensics, law, forensic science and cyber security, to provide students with a vast range of skillsets and competencies (Angelopoulou and Vidalis, 2015). Where, students should gain a sound understanding of forensic principles, methods of "preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence" (DFRWS, 2001).

Though, authors such as Thomas, Tryfonas and Sutherland (2009) observed that digital forensics programmes are largely based on generic computing curricula modified for computer forensics they found difficulties and uncertainties in decisions towards inclusion and removal of particular topics. Analysis by authors Irons, Stephens and Ferguson (2009) demonstrate how analysing courses enabled the categorisation of modules by "broad subject areas" such as "Digital Forensics", "Computer Science", "Law", "Forensic Science" etc. Where authors have stressed how the focus of such curricula is placed on the "life-long learning and the digital forensics process rather than about the tools", categorising modules by their multi-disciplinary nature, e.g., "Digital Investigation", "Computer Technology", "Criminal Justice" and "Other Courses" (Kessler and Schirling, 2006, p. 3). While such examples provide insight towards the outline of course structure and design, they do not provide an in-depth review of current course offerings, content, nor a conceptual framework.

A paper titled 'Digital Forensic Trends and Future' (Dezfoli *et al.*, 2013) looks at journal papers from 2008 to 2013 and is used as a comparable source to course analysis later in this section. The paper looks at keywords analysed "to obtain a view of recent interest in the arena of digital forensics" among research journals (Dezfoli *et al.*, 2013). Topics and terms such as 'Computer Forensics', 'Mobile Device Forensics', 'Network Forensics', 'Database Forensics', 'Multimedia Forensics', 'Cloud Forensics' and 'Other' were identified by Dezfoli *et al.* (2013). Furthermore, computer and network forensics were most popular with mobile and cloud forensics mentioned on far fewer occasions.

While this review highlights the need to capture qualitative responses from various stakeholders, this review must first look at current course offerings through review of documentation and identify common attributes across courses in the UK. Throughout this section several approaches are used to gather information including literature review, document gathering and analysis in addition to the collection of data from external providers[4].

This section looks at 32 existing programmes found in 2017 where a review of their curriculum content (e.g., modules, credits and core/optional titles) was conducted using UCAS webpages and readily available course documentation. Of the courses identified, 32 were directed at forensics and security; 14 were solely digital forensics (e.g. forensic computing or computer forensics), 13 focused on security and forensics combined. The remaining five were computing, or computer science with forensics, security or networking, or focused on policing studies and cybercrime[5].

As identified in section 2.2 course naming conventions and descriptors can be broad, brief or ambiguous which can lead to incomplete information and can provide uncertainty for a range of stakeholders. However, analysis of details from courses collected focused on keywords associated with digital forensics and cyber security across module naming conventions. These keywords came from searches through literature to discover prominent categories. In particular, Karabiyik (2015, p. 11) who denotes four “digital forensics branches”: computers, networks, databases and mobile technologies. Table 2.3 depicts keywords and themes found among programmes reviewed, albeit not an exhaustive list. The left column represents all keywords with a count of 10 or above, while the right column presents those identified less frequently. Results demonstrate the top three commonly identified keywords among module titles are: ‘Forensic’, ‘Security’ and ‘Network’.

When looking at the data gathered (e.g. course details and module titles) there were approximately 41 modules with broad naming conventions such as, ‘Digital Forensics’, ‘Digital Forensic Investigation’, ‘Digital Forensic Analysis’, ‘Computer Forensics’, and ‘Advanced Computer Forensics’. The uncertainty of what may be included in these modules could explain the limited information on a special interest topic such as, mobile forensics within HE digital forensics. The first year of study at many universities offering digital forensic courses were observed to be relatively similar to their computing counterparts with many

[4] Data relating to all course can be found in Appendix C.

[5] This review also considered a few other courses which were advertised as computer science with elements of security which can be found in Appendix C - C.7.

opting for one or two modules which were aligned to forensics or security. It is believed that this is due to the necessity for learning the underlying foundations of computing such as, computer systems, operating systems and so on before progressing with defining the skills and abilities for a more specialised subject.

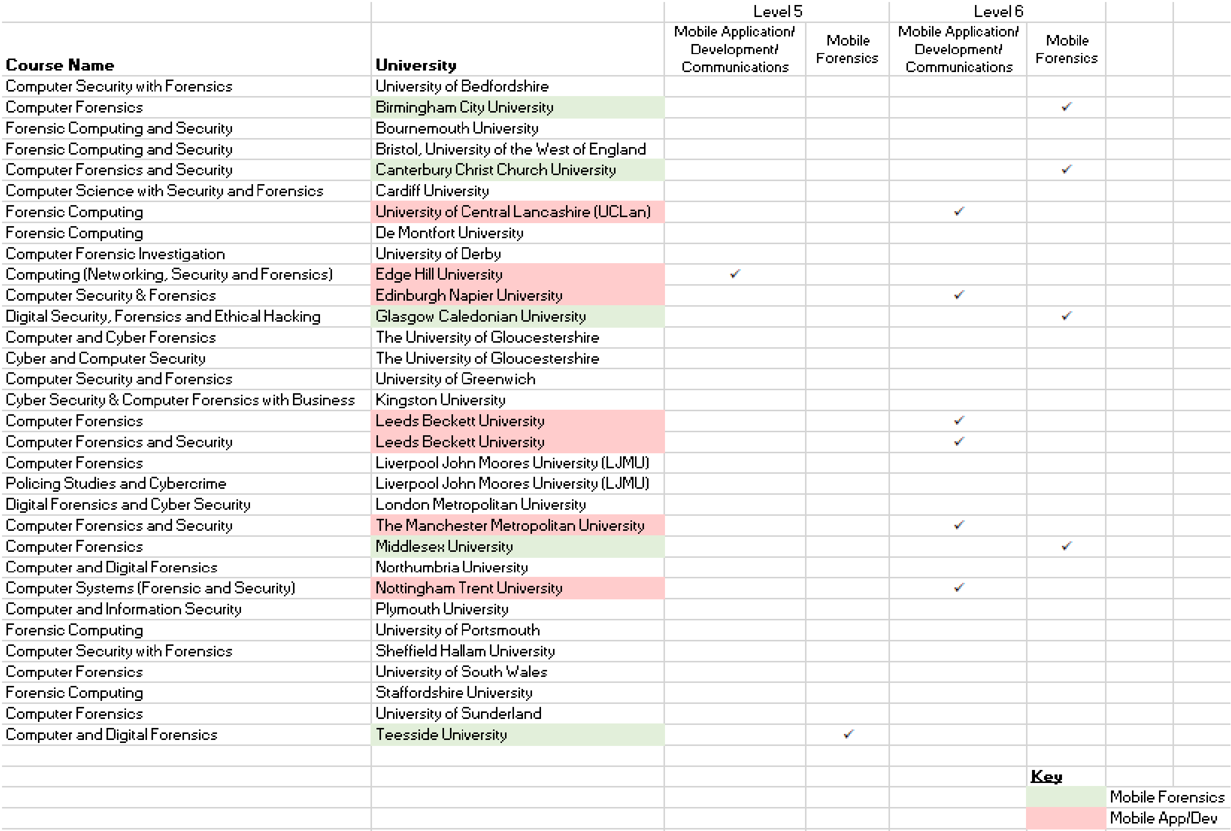
Keyword	Count
Forensic	96
Security	77
Network	74
Project	53
Programming	48
Development	38
Database	32
Professional	32
Web	31
Advanced	31
Placement	28
Management	27
Investigation	24
Fundamentals	23
Analysis	19
Software	18
Operating Systems/OS	19
Ethical Hacking	14
Mobile	12
Computer Systems	12
Crypto	11
Law	11
Penetration Testing	9
Internet	9
Issues	9
Business	8
Math	8
Modelling	6
Cloud	5
Tools	5
Research Methods	4
Systems Analysis	4
Human	4
Legal	3
Study	3
Web Technologies	3
Web Programming	2
Emerging	2
Contemporary	2
Live Forensics	1
Games	1
Systems Design	1
Virtualisation	1
E-Discovery/Disclosure	1
Artificial Intelligence	1

Table 2.3 – Popular Course Module Offerings on Digital Forensic/Cyber Security Courses in 2017: A Keyword Search

It is not surprising that the most common words associated with modules relating to digital forensics are forensic, security and networks. Authors such as, Cigoj and Blažič (2016, p. 15) recognise that the work of a digital forensic practitioner is complex, most often due to "the nature of the network technology applications and the speed of technological changes in the area of cybercrime … a challenge that is not always well addressed". This is an interesting point, where analysis of course modules supports this claim in the essence that network forensics for example, was not specifically mentioned in course titles. While networking was a keyword, Network Forensics/Investigation was only noted on one course at level 4 and one at level 5, suggesting that the fundamentals of computing and networking are the main initial focus of programmes in the first and second-year studies. Which leads back to the reliance and development programmes adopt from and share with regular computing degrees. It is only progression into level 6 studies where networking and its applicability within digital forensics were mentioned on ten courses.

What is also surprising is how Mobile Forensics and Mobile Application/Development were reflected less frequently in module titles particularly on digital forensic courses. Just six institutions (seven occurrences) included mobile application/development in modules available; however, only five institutions include mobile forensics where two were courses which focus on forensics and security combined (demonstrated in Figure 2.3). Tu *et al.* (2012, p. 21) note that from a survey of practitioners the type of cases they were involved with were those involving mobile devices: "55.6% of overall cases, involve mobile media". In late 2017, this proved ever more prevalent when a report by Big Brother Watch (2017, p. 4) showed that from nine UK police forces, data was extracted from "95,143" mobile devices during investigations, approximately 61% of devices. Traditional computers and laptops accounted for approximately 24% (Big Brother Watch, 2017, p. 4).

The question which must be asked here is whether the absence of newer technologies and forensic interests in course titles and descriptors is due to poor or limited promotion, or whether this reflects course alignment as still very much directed at traditional computer forensics. While the literature and course analysis cannot answer this question, the literature can highlight that topics such as mobile forensics have been mentioned as an important area for digital forensics education since as early as 2006 (Stephens and Induruwa, 2007). Therefore, it is alarming that few courses in 2017 promote this[6].



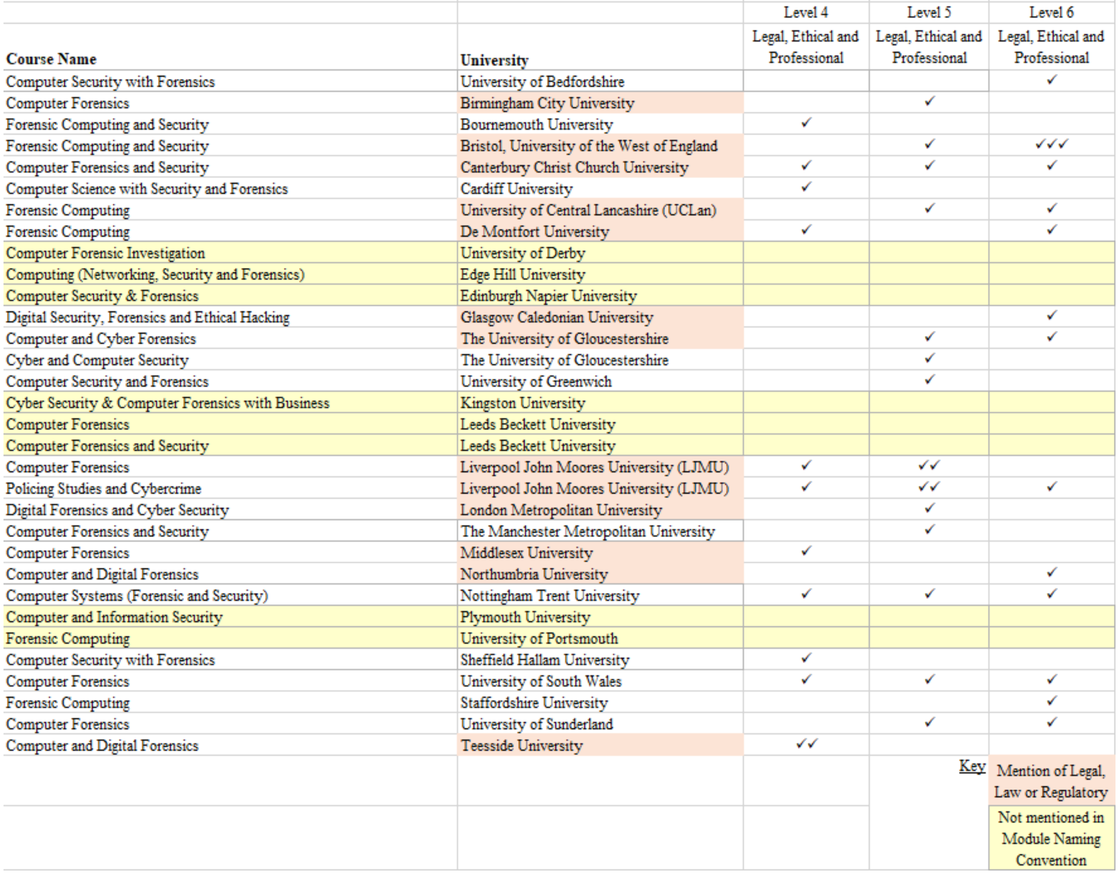
		Level 5		Level 6	
Course Name	**University**	Mobile Application/ Development/ Communications	Mobile Forensics	Mobile Application/ Development/ Communications	Mobile Forensics
Computer Security with Forensics	University of Bedfordshire				
Computer Forensics	Birmingham City University				✓
Forensic Computing and Security	Bournemouth University				
Forensic Computing and Security	Bristol, University of the West of England				
Computer Forensics and Security	Canterbury Christ Church University				✓
Computer Science with Security and Forensics	Cardiff University				
Forensic Computing	University of Central Lancashire (UCLan)			✓	
Forensic Computing	De Montfort University				
Computer Forensic Investigation	University of Derby				
Computing (Networking, Security and Forensics)	Edge Hill University	✓			
Computer Security & Forensics	Edinburgh Napier University			✓	
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University				✓
Computer and Cyber Forensics	The University of Gloucestershire				
Cyber and Computer Security	The University of Gloucestershire				
Computer Security and Forensics	University of Greenwich				
Cyber Security & Computer Forensics with Business	Kingston University				
Computer Forensics	Leeds Beckett University			✓	
Computer Forensics and Security	Leeds Beckett University			✓	
Computer Forensics	Liverpool John Moores University (LJMU)				
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)				
Digital Forensics and Cyber Security	London Metropolitan University				
Computer Forensics and Security	The Manchester Metropolitan University			✓	
Computer Forensics	Middlesex University				✓
Computer and Digital Forensics	Northumbria University				
Computer Systems (Forensic and Security)	Nottingham Trent University			✓	
Computer and Information Security	Plymouth University				
Forensic Computing	University of Portsmouth				
Computer Security with Forensics	Sheffield Hallam University				
Computer Forensics	University of South Wales				
Forensic Computing	Staffordshire University				
Computer Forensics	University of Sunderland				
Computer and Digital Forensics	Teesside University		✓		

Key
🟩 Mobile Forensics
🟥 Mobile App/Dev

Figure 2.3 – Mobile Modules by Course in 2017

[6] A cautionary note based on the regular review of curriculum, there may be more course which include mobile forensics.

In addition to this, an interesting point to consider was the lack of legal associations with module titles. The terms ‘legal’ or ‘law’ and ‘regulatory’ only appeared on 14 occurrences. Of the 10 institutions which mentioned these terms in module headings, seven were solely digital forensic courses (Figure 2.4). These are particularly low counts among the courses represented. It may be argued that the legalities, ethical and professional issues accompanying digital forensics are intrinsic of all modules and learning (e.g., data recovery, data analysis, ethical hacking, computer security) and therefore there may be no need to include dedicated modules on such issues, thus not appearing in multiple module naming conventions. Others may argue that although legal and regulatory issues were once a staple module in a digital forensic course, focus nowadays must also be placed on regulations relating to corporate digital forensics. Furthermore, with the addition and shift towards cyber security flavoured courses the once traditional law enforcement drive to course learning may have been adapted with legalities and regulations being intrinsic through all content.



		Level 4	Level 5	Level 6
Course Name	**University**	Legal, Ethical and Professional	Legal, Ethical and Professional	Legal, Ethical and Professional
Computer Security with Forensics	University of Bedfordshire			✓
Computer Forensics	Birmingham City University		✓	
Forensic Computing and Security	Bournemouth University	✓		
Forensic Computing and Security	Bristol, University of the West of England		✓	✓✓✓
Computer Forensics and Security	Canterbury Christ Church University	✓	✓	✓
Computer Science with Security and Forensics	Cardiff University	✓		
Forensic Computing	University of Central Lancashire (UCLan)		✓	✓
Forensic Computing	De Montfort University	✓		✓
Computer Forensic Investigation	University of Derby			
Computing (Networking, Security and Forensics)	Edge Hill University			
Computer Security & Forensics	Edinburgh Napier University			
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University			✓
Computer and Cyber Forensics	The University of Gloucestershire		✓	✓
Cyber and Computer Security	The University of Gloucestershire		✓	
Computer Security and Forensics	University of Greenwich		✓	
Cyber Security & Computer Forensics with Business	Kingston University			
Computer Forensics	Leeds Beckett University			
Computer Forensics and Security	Leeds Beckett University			
Computer Forensics	Liverpool John Moores University (LJMU)	✓	✓✓	
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	✓	✓✓	✓
Digital Forensics and Cyber Security	London Metropolitan University		✓	
Computer Forensics and Security	The Manchester Metropolitan University		✓	
Computer Forensics	Middlesex University	✓		
Computer and Digital Forensics	Northumbria University			✓
Computer Systems (Forensic and Security)	Nottingham Trent University	✓	✓	✓
Computer and Information Security	Plymouth University			
Forensic Computing	University of Portsmouth			
Computer Security with Forensics	Sheffield Hallam University	✓		
Computer Forensics	University of South Wales	✓	✓	✓
Forensic Computing	Staffordshire University			✓
Computer Forensics	University of Sunderland		✓	✓
Computer and Digital Forensics	Teesside University	✓✓		
			Key	Mention of Legal, Law or Regulatory
				Not mentioned in Module Naming Convention

Figure 2.4 – Legal, Ethical and Professional Modules by Course in 2017 (excl. Placement and Practice)

Considering this, modules relating to legal and ethical aspects of digital forensics and professional elements were grouped during review and while the specific contents of these modules is unknown, they appeared at 11 institutions (12 occurrences) across level 4, with many institutions concentrating on the delivery of these at level 5 (12 institutions/16 occurrences) and level 6 (13 institutions/15 occurrences) as depicted in Figure 2.4 and Table 2.4. Modules include, for example, ‘Business and Professional Issues’, ‘Professionalism in

Forensics and Security', 'Ethical and Professional Issues' as well as 'Professional Skills'. Further analysis into the professional topics included across these courses show that the majority were associated with the practitioner as a professional and their skills (10) and professional development (11) (Table 2.4). These modules are often used to educate students on practitioner and real-life experiences to develop their skills and abilities when fitting in to the workplace and conducting digital forensics or cyber security activities.

		Keyword Count across Courses		
Keyword		L4	L5	L6
Legal	*Legal*	1	1	1
	Law	2	7	2
	Regulatory	1	0	1
Professional	*Development, Practice & Management*	2	4	4
	The Professional & Skills	1	5	5
	Professional Issues	0	3	1
	Ethical & Professional Issues	1	1	2
	Placement & Experience	0	0	3

Table 2.4 – Legal, Ethical and Professional Modules by Course in 2017

A similar study which emerged after this review was conducted presented by Dafoulas, Neilson and Hara (2017, p. 149) demonstrates similar results in the courses they examined, finding that only 11 institutions "offered a module that covered legal and regulatory issues". Dafoulas, Neilson and Hara (2017, p. 149) note how half of the programmes were inclusive of modules relating to regulatory issues at level 5 and 6, however, identify that it is still "quite an omission" due to the importance of 'Legal and Regulatory Issues'. Identifying these as an 'omission', i.e., the action of excluding something, or a failure to fulfil an obligation (Oxford University Press, 2004), is quite a bold statement where analysis of course content is infeasible and difficult; however, Dafoulas, Neilson and Hara (2017, p. 149) do highlight that such issues may be covered in other modules. The paper comparable with this review illustrates that "… Level 4 [studies] … were often quite generic in nature and sought to provide a general introduction and background to different major areas in computing" (Dafoulas, Neilson and Hara, 2017, p. 149). Topics such as programming, networking, hardware and architectures, databases and, professional issues and development were found to be the most popular across level 4 studies during an examination of 29 UK programmes explored by Dafoulas, Neilson and Hara (2017, p. 149). Drawing to attention the "suggest[ion] that [these] represent the core topics of knowledge for anyone seeking to become a practitioner in this field" (Dafoulas, Neilson and Hara, 2017, p. 149).

Dafoulas, Neilson and Hara (2017, p. 150) also recognise that topics such as Network Forensics and Mobile Forensics are inclusive in only nine of the courses they examine, of which there were twenty-eight.

However, the work of these authors show some discrepancies whereby, the authors list 31 available courses in the UK and state their analysis is based on 29 HEIs while only demonstrating 28 courses in their data analytics (Dafoulas, Neilson and Hara, 2017). Additionally, literature presented by Dafoulas, Neilson and Hara (2017, p. 154) reveals Canterbury Christ Church University does not include mobile forensics on their Computer Forensics and Security course. The author of this thesis can confirm that mobile forensics has been longstanding within the previously named Forensic Computing degree and the revalidated Computer Forensics and Security course present modules named 'Digital Forensics and Ethical Hacking' or 'Forensic Computing Investigation 3' which reflect a wider breadth and depth of topics. Observations can be made that these titles do not reflect the entire contents of the module such as, mobile forensics, programming/scripting, report writing, or Mac and Malware forensics. Similarly to the results published by Dafoulas, Neilson and Hara (2017) this demonstrates there is the need for continuous reflection, clarification and updating of course briefings as well as content, delivery and development.

Another special interest topic: Cloud computing and technology, were mentioned at 5 institutions. This is particularly surprising where the development within computing and everyday life has seen a reliance on cloud-based technologies, at minimum for data backup and storage. Dlamini, Venter and Eloff (2014, p. 244) depict problems associated with cloud-based investigations drawing to conclusion such investigations extend past the traditional forensic computing approach. The traditional forensic computing approach is well-founded among long-standing digital forensics education. Thus, the greater pro-active approach which Dlamini, Venter and Eloff (2014, p. 245) state is required of cloud-based forensics may make argument against its delivery within current education due to demands on staff resourcing, time and cost efficiency to deliver such practice as well as plausibility. However, again, this review can only observe that such a topic is not promoted in many course descriptors and may recognise that such content may be included in, for example, networking, investigation, data recovery or analysis modules.

Other topics linking to cyber security and information security which are sought after within industry such as vulnerability assessment, malware and threat and risk assessment analysis are also considered (Potter and Vickers, 2015). In a search for 'vulnerability' in the listed module names, one course consisted of a module named 'Penetration Testing and Ethical Vulnerability Scanning'. However, in a search for 'Penetration Testing' 9 occurrences were found. In a search for 'risk' results found two institutions including one module each (one at level 5 and one level 6) which included the terms 'security and risk'. Taking a much broader approach, the search for 'Ethical Hacking' resulted in 14 occurrences, 'Cyber Security' in 5 occurrences, 'Computer Security' in 7 occurrences, 'Information Security' in 6 occurrences. When looking for 'malware' this topic occurred at three different institutions all of which appeared at level 6 study. Again, what this analysis cannot affirm is the exclusion of these topics across all courses. As mentioned previously with CCCU, students cover aspects relating to malware analysis in a module in their level 6 studies although this is not replicated in the module naming convention. This thesis can only say that courses may or may not include such content under broader module naming conventions.

What is also interesting are the limited addition of new topics, much of this review has found programmes to be centred on the underpinnings of computing programmes, Dafoulas, Neilson and Hara (2017, p. 150) explain in their own findings that new topics can provide students with unique attributes and skills for employability in the sector. At the time of writing there is a trend around AI and the Internet of Things in digital forensic and cyber security research. In a Google Trends search for Artificial Intelligence as a Topic and Search Term, results found that there had been a rise in the search for the topic since 2016 (Google, 2019a). As for the Internet of Things, there has been a steady rise of the search for the Topic and Term since 2013 (Google, 2019b). While many authors such as, Irons and Lallie (2014) and Mitchell (2014) have discussed the application of AI and the importance of intelligence within digital forensics.

There have also been numerous papers published on IoT and digital forensics and cyber security which highlight the challenges posed by such technologies (Hegarty, Lamb and Attwood, 2014; Hossain, Fotouhi and Hasan, 2015; MacDermott, Baker and Shi, 2018). The same can be said in the application to cyber security where technologies such as IoT, AI and cloud computing are enablers to new value in business but also pose a loss in economic value due to security risks and cyber-attacks on businesses. Nevertheless, degree programmes are yet to reflect these trends and may reflect issues with measures in the move for digital forensics and cyber security to keep pace due to the “changing landscape of crime” (MacDermott, Baker and Shi, 2018).

With this, the search for ‘emerging’ which found just two HEIs included in a module and ‘developing’ which led to four occurrences all applying to databases, and e-commerce/mobile applications. What cannot be concluded here is the inclusivity of new and emerging technologies within course programs. From first glance it may seem like these are excluded where focus is still seemingly mainstream computing and computer (i.e. desktop/laptop) forensics. However, this cannot be ascertained across all courses without analysis of each module contents (e.g. lecture, lab, extra curricula content) or by providing all students across the UK having studied a course in digital forensics the opportunity to critically evaluate at a profound and meaningful depth their course, content and learning. This is an unrealistic task for this review and this thesis, and which is unlikely to be conducted to such scale.

Full course data used during review/analysis are depicted in tabular format for each level of study in Figure C.6.1.1 to Figure C.6.3.3, where each tick represents a single module[7]. Furthermore, the following key results were found:

- Unsurprisingly, Investigation and Analysis appeared on 24 and 19 occasions respectively; both are crucial elements of a digital forensic and a cyber security practitioner's daily role
- Computer/Operating Systems (grouped during data collection) appeared across 19 HEIs, appearing on 12 instances at level 4
- Databases were mentioned on 14 occasions at level 5 across 10 courses and on 8 occurrences at level 6 study; showing to be a key component of any computer forensics or security course
- Web/Web Development were combined and appeared at 13 institutions (level 4), six institutions (level 5) and seven institutions (level 6); 16 institutions of the 32 did not mention web/web development in module titles across any of the three levels of study
- Networking was specifically mentioned within 14 module titles at level 4. Many programmes opting to include networking as a specialised subject in levels 5 and 6
- Project appears on 53 occurrences across the 32 courses with each course including a project or study in the final year, where five courses also include a dedicated module for a group project
- Programming was found in all courses where introductory and fundamental elements of programming for the students were found in the first year of study (level 4)[8]
- Internet (9 occurrences), Artificial Intelligence (1 occurrence) and e-Discovery (1 occurrence) are seen at very few institutions and may be relatively new additions as dedicated modules
- 23 of the courses include an option for a placement year; in other examples courses offer placement modules (2 institutions) or include placement opportunity preparation modules (2 institutions).

Review of course programmes and the literature within this section have fostered reflection on how course content is not readily identifiable, and successes are unfounded. While research by Norman and Williams (2016, p. 198) is based on policing degrees the authors discuss how "there is limited evidence on officers' own perception of how education is received by the organisation and their colleagues, despite a large number of officers going through a variety of police related education every year in the UK" (Norman and Williams, 2016, p. 198); the same can be said for digital forensics. While digital forensics education in the UK has seen a rise in the last decade, there is little narrative nor evidence of professionals nor graduates

[7] For example, Figure C.6.1.1 shows that on seven courses there are two programming modules (two ticks) at level 4 study. Please see Appendix C for full tabular data.

[8] At the time of analysis there was only one course which did not include an element of programming along with, an element of networking. This course focused more on police studies and investigation with cyber-related content although, this looks to have been revised in the most recent course offering.

and students perceptions and views on the reception of digital forensics education in industry, much of the literature focuses on learning within the domain and echoes issues expressed by 'cyber forensic' professionals including those describe by Harichandran *et al.* (2016), including:

- the need for greater opportunities for education, training and certifications within the discipline or business;
- a need for greater knowledge and skills alongside the knowhow of how to use specific tools; and,
- directed attention to the outdatedness of legislation and need for clarity.

2.4 Learning in Digital Forensics Education

Academically, the debate for, and use of both 'education' and 'training' in computer-related curricula, has been a recurring topic. This is contrary to professional environments where mostly training dominates. A strong distinction is made between education and training, where pedagogically, 'education' can be defined as "learning theory" (Rickman, 2004). Here fundamental knowledge is reinforced, and a much deeper mindset attained. Specific attributes such as self-directed learning, an inquisitive, open-minded and critical nature are required to successfully learn and actively engage in any given subject. 'Training' on the other hand involves acquisition of very subject-specific skills used to carry out specific tasks (Barnes, 2014). The training process could be seen to plot a short-term development curve to achieve successful skills. Similar techniques can be utilised in both education and training, but can also have very different goals and outcomes (Tong, 2004, p. 132). Irons, Stephens and Ferguson (2009, p. 86) identify that both practices complement the role of a digital investigator, where elements of digital forensics syllabi require both knowledge and skills.

Within digital forensics, training can be demonstrated through acquisition of short-term taught skills that one would require to use forensic-specific software such as EnCase (Guidance Software, 2015) and Forensic Toolkit (FTK) (AccessData, 2015), two of the most widely used computer forensics tools in the industry. Yasinsac *et al.* (2003, p. 5) state "it is not essential ... [to] understand the internal operation of the tools ... but what the tool reveals about the data and its underlying structure." Education can bring elements of this to the table, allowing for a more in-depth theoretical approach to deep seeded learning. Learning to some degree, how the tool can work internally is usually accomplished through the use of open-source digital forensics tools such as The Sleuth Kit (TSK)/Autopsy (Carrier, 2015) and Digital Forensics Framework (DFF) (Baguelin *et al.,* 2013). Similarly, programming languages rooted into computing degree programmes are usually an aspect of training and education.

Adelstein, Gao and Richard III (2005) and Garfinkel (2010) discuss training problems noting that much of the data relied upon, and its delivery, lack a degree of complexity and realistic nature where many courses rely on small training data. It can be seen that much larger investigations reveal lengthy imaging and processing times, therefore smaller datasets provide the supplier with more time to train individuals (Roussev, Quates and Martell, 2013, 2013; Meister and Chassanoff, 2014). However, the technical requirements to handle more representative quantities of data necessitate sufficient processing power and larger than normal storage capacities to manage imaging, searching, analysing and storing of the data. Very similar to training materials, many academic environments will utilise evidence files, usually, of a much smaller scale than that of a real-life investigation.

The main objective of any undergraduate degree is to prepare students for employment in their relevant industry. Within digital forensics a mix of education and training can be seen to fulfil requirements and business needs, such as proficiency in use of commonly used tools, and yet theoretical understanding of complex tasks and practices (Huebner, Bem and Cheung, 2010, p. 10). Such proficiencies also lead to the contrasting question, commercial versus open-source software and which is best for students' learning, engagement and understanding? As articulated by Huebner, Bem and Cheung (2010, pp. 10–11) open source tools provide much greater opportunity for a students' learning, providing the ability to develop packages, examine and analyse the tool, code and results appreciating complexities and importance. Huebner, Bem and Cheung (2010, p. 10) state that for a long time there has been a "dilemma faced by educators" in the decision over "commercial [and/or] open source" software.

There are also many challenges that can be associated with learning; key characteristics include student engagement and their drive to learn, as well as the quality of tutor performance and class content. Rawlings, White and Stephens (2005) note that higher education adopts an "enabling strategy", a learner-centred style focussing on learning through practical involvement which has led to Problem-Based learning (PBL) within disciplines. While no student learns the same way, learning styles become an important aspect of curriculum development. Within digital forensics, professional and real-life scenarios adopt a practical and hands-on approach in order to keep up-to-date with technological demands, similarly these approaches are adopted in education to enable theory-practice links.

While Nordhaug (2013) notes there are two ways of how learning styles can be observed; "user learning style[s]" and "the way to present the knowledge to learners", the scope of learning has varied and widened over time, with attributes such as 'e-learning' and 'distance learning' (Kessler, 2007; Chen, Hu and Shi, 2009; Nordhaug, 2013; Carter and Coupland, 2014); "Problem Based Learning (PBL)" (Watson and Fang, 2012; Irons and Thomas, 2014), and 'gamification' (Brennecke and Schumann, 2009; Muntean, 2011;

Kapp, 2012; Nagarajan *et al.*, 2012; Pan *et al.*, 2012; Hamari, Koivisto and Sarsa, 2014; Pringle and Potter, 2014; Pan, Schwartz and Mishra, 2015) to name but a few. Nance, Armstrong and Armstrong (2010, p. 7) identify multiple learning mechanisms, noting that case studies provide an opportunity to apply a "practical application to knowledge and skills". The complex nature of the subject influences teaching and learning, where authors state that "[i]n the current piecemeal situation gaps are clearly evident and a more holistic educational model is needed", identifying this as by no means a small task (Nance, Armstrong and Armstrong, 2010, p. 7).

Biggs (1999, p. 59) identifies that there is a higher level of engagement in active learning approaches such as PBL. PBL was first introduced within the Faculty of Medicine in the late 60s (Norman, 2008, p. 61). It is a learning mechanism which is clarified and developed in theory and practice as active learning due to its promotion and satisfaction of self-directed learning, facilitation by tutor, collaboration and contextualisation (Thomas *et al.*, 2016, p. 77). The idea behind PBL is for the student to use pre-gained knowledge and their cognitive skills effectively and efficiently in the application of a real-life scenario to develop their learning, depth of knowledge and to evaluate how they learn (Barrows, 1988).

Atypical of traditional teacher-centred methods such as lectures, seminars, and practical laboratories where the teachers' sole purpose is to pass on information. The teacher or lecturer is, therefore, a tool for facilitation, a tutor and guide for learners. Thomas *et al.* (2016, p. 77) epitomise this stating during PBL methods, students are divided into groups where they are then "presented with a case … [and] guided by a facilitator", however, they are expected to manage and define their own learning and objectives. This allows students involvement in their own learning process, adopting the "enabling" approach discussed by Rawlings, White and Stephens (2005). PBL implementation also allows for feedback from students which may often be pursued through qualitative or quantitative evaluations.

Nevertheless, literature has shown that there are issues noted with the implementation of PBL; for example, student uncertainty on what is expected during the problem and essences of feedback (Kay *et al.*, 2000, p. 121). Barrows (1988) professes that a lecturer's position is to facilitate skills such as problem-solving, critical thinking and self-directed/independent learning within PBL tasks. While Watson and Fang (2012) continue to state that a facilitator should look to encourage students, focus their attention, and provide questions which seek information and clarification from the learners. Other affects have been that of the tutor as an observer, or observers in the room, and how they can play a role in the performance of a student and pose educational challenges where the student feel "they [are] being watched" (Irons and Thomas, 2014, p. 8). However, such observations can provide valuable feedback for the students' development of learning (Irons and Thomas, 2014, p. 9); while, also allowing for the development of teachers' awareness to their own strategies, requirements, behaviours, mannerisms and their effect. Tryfonas (2008, p. 183) identifies that introductions of

> “practical skills via an interactive, cohesive and meaningful environment creates the potential for a higher degree of student engagement ... [where] the instructor can set learning objectives against requirements that stem from the professional field”.

Application within digital forensics demonstrates how PBL has been successful in the development and progression of student learning; including works by Irons and Thomas, 2014 and Govan, 2016. For example, to “help students understand the processes of digital crime scene analysis and search and seizure procedures ...to give them the opportunity to put into practice their digital forensics techniques” (Irons and Thomas, 2014). Works have also shown how PBL initiated in the domain of cyber security for student learning and engagement have been fruitful e.g., competitions, capture the flag events and so on (Irons, no date; Floyd and Yerby, 2014; Pusey, Gondree and Peterson, 2016). Implementation has seen well-thought out tasks involving ill-structured and real-world problems where attention is placed on a student-centred approach, developing generic problem-solving skills pursued through identification of a problem and cognitive processes (Kay *et al.*, 2000; Kessler, 2007; Watson and Fang, 2012).

Figure 2.5 depicts an example approach to PBL identifying key aspects of the PBL process outlined by Barrows and Myers (1993), cited in Savery and Duffy (1995) including, feedback and evaluation, defining the problem and clarifying ideas as well as sharing information and reflection.

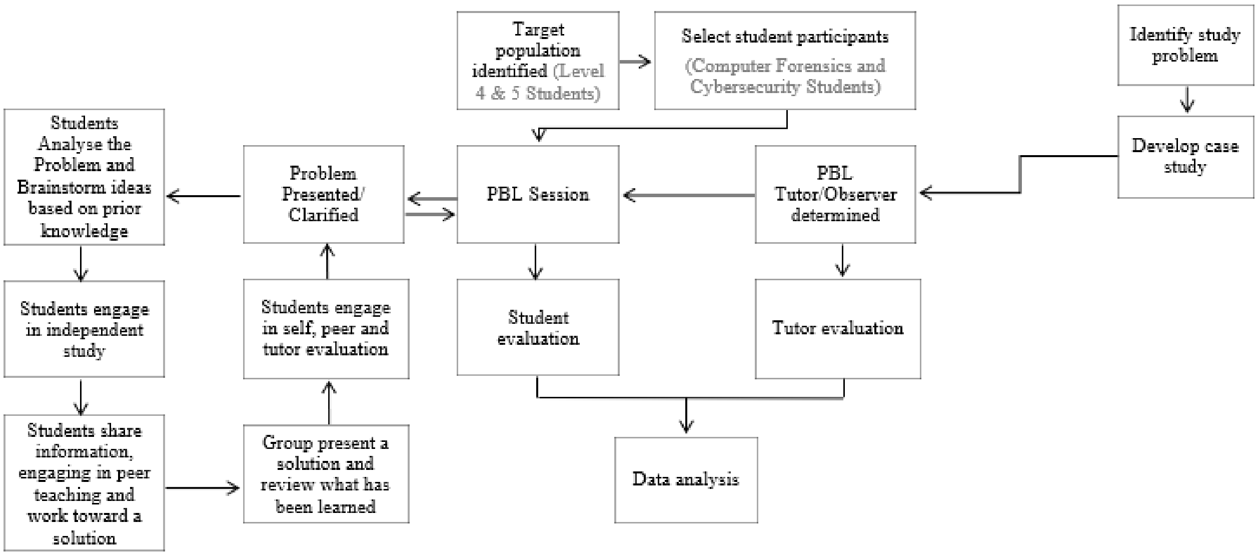

Target population identified (Level 4 & 5 Students)
Select student participants
(Computer Forensics and Cybersecurity Students)
Identify study problem
Develop case study
Students Analyse the Problem and Brainstorm ideas based on prior knowledge
Problem Presented/ Clarified
PBL Session
PBL Tutor/Observer determined
Students engage in independent study
Students engage in self, peer and tutor evaluation
Student evaluation
Tutor evaluation
Students share information, engaging in peer teaching and work toward a solution
Group present a solution and review what has been learned
Data analysis

Figure 2.5 – An example Problem-Based Learning approach

While learning in digital forensics has seen courses offering a mix of theoretical and practical, often problem-based, learning this raises the question of how the discipline can learn from other disciplines which rely on the theoretical understanding but are largely practical within industry. For example, disciplines such as education and medicine have a longstanding experience in producing vast numbers of experienced practitioners (fully qualified and trained) to progress through careers within the industry.

2.4.1 Learning from other disciplines

Taking medical education as an example which has existed for centuries, with practices continuously being based on practical experiences as well as large quantities of theoretical text (Segre, 2015). Books were used in primitive years when passing from generation to generation of physicians, however, practice truly developed the learning and knowledge that exists today. Today the road for medical developments and education has led to more scientific approaches as well as, established well-defined higher education programmes, encompassing both theory and practice. This is a highly practical and knowledge-reliant discipline that both digital forensics and cyber security could learn lessons from.

Learning, progress, improvements, knowledge and more within such a subject is a lengthy process, taking students several years to receive their degree in medicine and to specialise, a keyway to how the UK health system functions and produces new professionals. Nurses are trained at an undergraduate level, ensuring they have the industry experience within hospitals as well as the theoretical knowledge behind the complexities of health issues, handling patients and visitors and treatment of a range of patients. The nature of medical education can be outlined in a six-step approach identified as by Thomas *et al.* (2016, p. 7) which are used to provide “a logical, [and] systematic approach to curriculum development” to achieve the aims, goals and obligations of the educational programmes (Thomas *et al.*, 2016, p. 5). Similarly, to digital forensics, methods such as case study-based learning, problem-solving and other methods can be adopted to develop the skills of the targeted groups as well as assess and learn through numerous methods. However, where digital forensics can learn from medical education is the idea of clinical placements. Within medical education supervised practice in situations including teaching hospitals, health centres, private clinics and specialist services are a necessity for students.

It is suggested that these situations allow students to ponder a range of important career decisions, learn several skills, professionalism, network with experienced practitioners and placements can provide greater satisfaction with their course (Littlewood *et al.*, 2005). These environments also allow the students to learn on-the-job and understand how the day-to-day workings and tasks within medical settings are carried out and “develop theory-practice links … offer[ing] … enhanced learning experience in both practical and academic domains through a symbiotic relationship between the two” (Yiend *et al.*, 2016, p. 2). Studies such as that by Rawlings, White and Stephens (2005) identify that placement-based learning in Information Systems has significant academic and learning benefits. Though the authors identify a number of contributing factors and issues towards the adoption of placements within UK higher education (Rawlings, White and Stephens, 2005).

Within digital forensics education it has been noted that "a close relationship with the law enforcement community has been imperative to maintaining relevance and addressing an important national need" (Kessler and Schirling, 2006, pp. 8–9). This has been particularly important where placement opportunities have been impossible. Although, authors such as Salt, Lallie and Lawson (2011) and Lallie and Day (2012) note that in general, expectations, objectives and "[c]areer structures and progression pathways are not as clearly defined as they may be in other industries"; this to some degree owing to the youth of digital forensics. Digital forensics education has similar traits to medical education (e.g., the strong bond between the need for theory and practice and the heavy reliance on experience as a contributing factor toward professional development) where, necessary placements within digital forensics education could provide students with attitudinal advantages as well as enhanced learning of the subject matter and importance for multidisciplinary working within the sector.

2.5 Why focus on the UK?

This review has considered the UK higher education system at undergraduate level, largely due to the number of courses that have been introduced over the years. While there has been some research about curriculum design, development, and delivery in the UK, as discussed above, there has been little to no exploration of the challenges, experiences, and ideals outside of the academic stakeholder group. Some studies have considered the challenges faced by professionals and the relation to training for example works by authors such as Irons, Stephens and Ferguson (2009); Lang *et al.* (2014); Karie and Venter (2015); and Vincze (2016). However, stakeholders such as students, graduates and further narratives from professionals have not been explored. The literature has also seen works largely exist in countries such as the United States and Australia, yet academic programmes in digital forensics are offered in several other countries including, Canada, Ireland, Germany, Netherlands, Norway, South Africa, and India. So, why the focus on the UK, and to what extent is the UK a leader in addressing digital forensics in higher education? Arguably, much of the research in digital forensics has come from authors based in the United States and the United Kingdom. Furthermore, there are a vast quantity of courses on offer across America. However, of the countries mentioned in Europe, the UK leads by number of courses available and, as the literature suggests, has been designing, developing, and delivering courses since the early 2000s. The number of courses available may not address how the UK is a leader, though it provides opportunity to explore content included in the courses today, as demonstrated above. The explosion of courses in the UK and challenges/experiences documented by authors in existing research also allows for comparison to the last decade regarding the design and delivery today. These comparisons may be useful in identifying improvements required within the field to further develop educational offerings and combat existing challenges considering the ever-evolving field and the abundance of potentially new challenges the field may face in the years to come. In addition, there is little by way of an overall international standards within digital forensics or digital forensics education. Prior to the ISO 17025 there were few international standards that could be applied to digital forensics, and still the standard is not without its problems. The current standard considers laboratory accreditation and compliance within the digital forensic process and includes, for example, validation of methods and procedures, validation, calibration and verification of tools, qualifications, and documenting and written procedures. However, it does not consider digital forensics education and while international research exists, there is still no agreed standard of education within the discipline. This review demonstrates that the field of digital forensics would benefit from a wider review of courses across the international space to identify the current context of educational programmes in other countries such as the United States. A review should consider if the challenges are comparable, relevant, and what improvements and collaborative effort can be made between countries, communities, and various stakeholders. The wider review should extend to training provisions available. However, this is outside the scope of this research which focuses solely on the UK as a provider of digital forensics education. Another motivation for the focus on the UK in this study was the researcher's own background having studied and working within the UK higher education system and interests in contributing toward the shaping of future digital forensics education.

2.6 Summary

This chapter has focused on existing literature and course analysis at the time of writing to identify key topics and potentials of digital forensics education. This review has highlighted how inadvertencies, difficulties in data collection and ambiguities central to acknowledging content in existing programmes reinforces the need for clarity from HEIs on programme content and promotion. The design of educational courses remains, to some extent, unquestioned for what makes an effective practitioner and what is expected of an individual with an educational background in computer forensics.

This review has also recognised that digital forensic courses must cover an exhaustive level of content and underlying computer skillsets which are required to deliver a practitioner for a range of stakeholders. While the ideals of a digital forensic practitioner may vary widely dependent on the view of various stakeholders and their own experiences, courses across the UK are seemingly providing at basic delivery the fundamentals of computing, networking and forensic analysis based on course and module titles. However, with the limited and broad information relating to the degree programmes the contents of these programmes is widely unknown and therefore their effectiveness and accuracy cannot be determined.

The literature considered within this chapter has set the scene and guided subsequent questions of this research identifying potential gaps among relationships between industry and academia alike where questions such as, *what is the student curriculum for digital forensics?* have been considered. The literature and review of courses has highlighted that while programmes have been outlined by several authors, there has been little by way of narrative to define and focus on the need to identify what makes an effective digital forensics practitioner.

This thesis therefore argues that by capturing qualitative responses from several stakeholders involved in academic/professional digital forensics that these viewpoints and experiences may allow academic courses to tailor programmes on offer to current, rather than perceived, topics, skills, needs and benefits of the student body they cater for and to ensure these are delivered going forward. Answering to some extent the question of *what makes an effective digital forensics practitioner?* Although, it should be documented that while course designs should be based somewhat on industry ideals and practitioner views and desirability's of the workforces they require, these must be balanced with necessary fundamentals and underpinnings such as those already covered within the research domain. For these reasons, qualitative responses and narrative of these views and experiences are the focus of results chapters in this study.

3. A Review of Academic Challenges for Digital Forensic Curricula

Introduction

Before looking at capturing and analysing qualitative responses, it can be recognised that there have been several arguments made where existing forensic investigative frameworks hold several shortcomings (Reith, Carr and Gunsch, 2002b; Yusoff, Ismail and Hassan, 2011). Often traditional methodologies and guidelines are described to be less than fit-for-purpose in more volatile and fragile evidence states which has led to what Du, Le-Khac and Scanlon (2017) describe as broadly similar approaches developed for multiple use case scenarios. Similarly, until recent years few standards or frameworks within digital forensics education have been available to aid information gathering for potential students or professionals seeking graduates for employment. This chapter further focuses on delivery of digital forensics and cyber security in higher education, with particular attention to the most recent introduction of standards and frameworks adopted in the UK, US and European Law Enforcement with regards to delivering curriculum for cyber security/cybercrime and additional digital forensics.

3.1 Digital Forensics: Is it an Academic Discipline

Universities within Western Europe exist dating back to the 12th century, where at that time disciplines such as Arts, Science, Medicine, Theology and Law were taught and practiced (Krishman, 2009, p. 31; Segre, 2015, p. 87). These subjects became what was known as academic disciplines. Since, the 19th century saw subjects within languages and social sciences formed, whereas the 20th century saw new disciplines such as education and psychology (Krishman, 2009, p. 32).

The concept of an academic discipline is, however, not straightforward and a concise definition is less than easy to define. An academic discipline uses the word ‘discipline’ to invoke the meaning: subject. Krishman (2009, p. 8) notes it to be “specific and rigorous scientific training that will turn out practitioners who have been ‘disciplined by their discipline’”. Krishman (2009, p. 9) goes on to discuss the phrase takes on the “technical term for the organisation of learning and the systematic production of new knowledge”; where, not all subjects are necessarily a distinct discipline solely because they are taught in the environment of a university or college. In fact, most academic disciplines known today have formed over many generations and usually have a distinct community with specific vocabulary and observe formal standards. To help formulate whether a subject is in fact a discipline or sub-discipline, Krishman (2009, p. 9) identifies six characteristics which would be adopted, in full or part:

1. "object of research"
2. "body of specialist knowledge (specific to the subject)"
3. "theories and concepts"
4. "specific terminologies or specific technical language"
5. "specific research methods"
6. "institutional manifestation … respective academic departments and professional associations".

— (Krishman, 2009, p. 9)

The transparency of defining what subjects constitute an academic discipline or sub-discipline is still often unclear. Krishman (2009, p. 34) notes that defining a new academic discipline involves having a clear agenda for research and definition of the subject. Grieb (1974, cited in Krishman, 2009, p. 35) highlights examples of how these were once relatively simple to distinguish. Increased overlapping of subjects, subject maturity and the need for innovation has often led to "overlapping fields [being] split from their parent disciplines and form[ing] a new discipline" (Krishman, 2009, p. 35). For example, the discipline of computer science has many branches which include subjects such as artificial intelligence, computer security and software engineering.

When discussing digital forensics and cyber security these are yet two further subjects which may be classified as sub-disciplines of computer science. However, the inter-disciplinary nature of these subjects may reflect the need to be classified as relatively new and distinct disciplines, particularly in comparison to longstanding subjects such as history and medicine. There is little research which discusses nor associates the six abovementioned characteristics with digital/computer forensics and its placement as an academic discipline. Unlike more traditional fields of study, there may be characteristics which digital forensics in higher education does not yet entirely fulfil; needless to say, this does not mean the six characteristics are not satisfied to some extent. For example, characteristic two: a body of specialist knowledge is the central underpinning of the discipline.

Digital forensics has steadily become an ever emerging science: defined as an "intellectual and practical activity encompassing the systematic study of the structure and behaviour ... through observation and experiment" with replicable results (Oxford University Press, 2015). As a field, digital forensics requires innovation, continuous experimentation and investigation. It is always changing, growing, developing and is a fast-paced specialist area with underlying fundamentals of not just computer science, the subject is highly technical and incorporates several specific terminologies and technical language which must be presented to a layperson for transparency and understanding.

Characteristics which may arguably immobilise the field from being defined as a distinct academic discipline are 1., 5. and 6 (above). Where the discipline suffers from struggles in areas of research; as an academic field it has grown at a steady pace with authors such as Garfinkel *et al.*, (2009) questioning the replicability of research in this field, and for many the science is still very much seen in its infancy stage. There are thousands of academic research papers which relate to digital forensics and several conferences which are dedicated to computer forensics and security; however, it is not classified as a historical academic discipline which often include a large base of long-lasting journals with high impact factors. Using journal rankings from Scimago Lab (2018) one can identify a handful of journals which still exist today and their totality is digital/computer forensics or security (Table 3.1).

	Impact	Scimago Metric			
Publication	Factor*		H Index	Coverage	
Computers and Security	2.65	CS	72	1982 –	UK
Digital Investigation	1.771	CS	39	2004 –	UK
The Journal of Digital Forensics, Security and Law	N/A	N/A	N/A	2006 –	US
International Journal of Electronic Security and Digital Forensics	N/A	CS	9	2008 –	UK
International Journal of Information and Computer Security	1.658	CS	9	2009 –	UK
International Journal of Digital Crime and Forensics	N/A	CS	10	2009 –	US
IEEE Transactions on Information Forensics and Security	5.824	CS	85	2006 –	US
*2017 H Index: metric to measure citation impact	CS = Computer Science				

Table 3.1 – Digital Forensic Journal Rankings based on Scimago Metrics

One journal, included in Table 3.1 has existed for over 30 years and is undoubtedly the most well-known within computing, however, its topic coverage is not solely digital forensics; similarly, to other journals, articles pertaining to digital forensics can be found among its volumes available. What these metrics show is the relatively low importance of some of these journals, however, it should be noted that scores are generally field-dependent and in this case, where a low number of journals are available or have survived, the highest-ranking journals in the table above may be classed as high impact scores. These rankings also demonstrate, again, the ill-defined position of digital forensics. For example, Scimago Lab (2018) lists the journal: Digital Investigation, as 190th inside the category Computer Science Applications with a calculated SJR score of 0.635. However, Google Scholar Metrics (no dateb, no datea) show that Digital Investigation ranks 6th within the category of Forensic Science.

While the subject exists at many institutions across the UK and USA, it is also not respective of its own department or professional associations; for which there are many and no one leader. There are arguments both for and against the distinctness of digital forensics and cyber security and it can be displayed that while the number of programmes on offer has increased there is still no real footing by which the discipline of digital forensics currently stands on its own. Digital forensics courses are seen in schools of Computing or Computer Science, Law, Policing, Criminology and Digital Technologies and more often tied with cyber security. Yet, the main aims of these degree programmes remains the same: to equip students with diverse yet fundamental knowledge and skills necessary to specialise in what are continuously expanding and highly technical industries.

Despite the role which digital forensics has played since its earliest incarnation, where standardised and essential principles, procedures and ethics as well as functional tools for practitioner use have been introduced, it has been unable to flourish in the same way within academia. Authors such as Irons, Stephens and Ferguson (2009, p. 89) identify that before the field can become its own discipline "agreement needs to be reached on issues surrounding discipline standards and boundaries – especially in terms of curriculum content, certification requirements, and accreditation expectations." The literature shows that there is no unique framework adopted which focuses on ensuring quality of digital forensics curricula and course offerings despite many universities outlining their academic programmes and key topic areas (Anderson *et al.*, 2006; Kessler and Schirling, 2006; Irons, Stephens and Ferguson, 2009).

3.2 A Review of Digital Forensics and Cyber Security Educational Frameworks

Vincze (2016, p. 186) states that "[t]he problem with a field like computer forensics is the lack of universally accepted standards that anyone can view and at least have an idea of the level of competency of the expert". This provides unique challenges in defining a curriculum and defining effective teaching, training of skilled practitioners. For example, identifying the skills required of such a practitioner and their effectiveness must take into consideration views of multiple stakeholders where, the term 'effective' signifies a greater and well-rounded set of questions and outcomes including areas of quality, administration, results, revenue and outcomes for those involved. While the literature (for example, Meyers and Rogers, 2004; Wolf, Shafer and Gendron, 2006; Karie and Venter, 2014, p. 1232; Lang *et al.*, 2014) demonstrate outlines of computer and digital forensic core modules at universities across the UK and US, there has up until most recently been a lack of frameworks centric to the digital forensic curriculum.

3.2.1 A lack of a widely accepted curriculum framework

Authors such as Lang *et al.* (2014), Meyers and Rogers (2004) and Strzempka (2010) reiterate that the lack of a defined, reviewed and widely accepted curriculum standards and framework leads to multiple problems when adopting and attempting to produce such a curriculum. Lang *et al.* (2014, p. 77) discuss "roadblocks to widespread adoption of" a single curriculum standard within digital forensics, noting that the main fall-back to such a proposition "was not the topic coverage, but the fact that they were difficult to implement at most institutions". Before this thesis commenced there were few works focussing on frameworks for digital forensics education a reason for this may arguably be the need for an authoritative entity to attract compliance and agreeance to boost implementation of such standards and frameworks.

While initial attempts included authors outlining courses and presenting challenges within the discipline, authors Wolf, Shafer and Gendron (2006) conducted a US study which showed initial attempts towards understanding the wider curricula and establishing a "preliminary conceptual framework" of attributes and dimensions common to multiple programmes. Although no framework was devised successfully and the study simply posed the question whether "digital forensics [is] a discipline/profession in an academic sense and if so, how should it be defined?" (Wolf, Shafer and Gendron, 2006). This was something highlighted previously in section 3.1 discussing whether the disciplines lack of educational framework and inter-disciplinary nature adds complexity to defining digital forensics as a distinct academic discipline.

According to Lang *et al.* (2014, p. 77) the challenges of curriculum standards development include:

> - "balancing training and education";
> - "lack of an adequate textbook on digital forensics";
> - "finding qualified faculty";
> - "lab setup";
> - "selecting appropriate prerequisites"; and a
> - "lack of widely accepted curriculum standards".
>
> — (Lang *et al.*, 2014, p. 77)

While the discipline has lacked a curriculum framework of its own, the majority of courses within the UK HE system have referred to multiple sciences and subject benchmark statements from the Quality Assurance Agency (QAA), mainly that of Computing (The Quality Assurance Agency for Higher Education, 2007, 2016). These benchmarks are used to describe the expectations and standards of a qualification and provide several attributes and capabilities deliverable from individuals at both technical and theoretical levels (The Quality Assurance Agency for Higher Education, 2007). Documentation provides students, academics and employers with a broad understanding of what skills and teachings undergraduates should have acquired on their computing courses and goes some way to understanding what an effective practitioner looks like. However, as the digital forensic industry grows, and more specialist personnel are required the question raised should include what makes an effective practitioner and what the academic discipline needs to provide beyond the standard computing curricula.

Rogers and Seigfried (2004) and Stambaugh *et al.* (2001) found that "education/training and certification were the most reported issue" when it came to a study of the digital forensic profession. Yet, no single body, organisation or regulator within the UK had been awarded the overall power to regulate or accredit digital forensic education. Accreditation and regulation within the profession has raised many issues and questions over the years, with widely differing views from a range of stakeholders. Examples have included debates central to the need for certifications versus qualifications where individuals have vocalised how certifications provide practitioners with "a whole alphabeti-spagetti soup of letters after their name" and do not infer knowledge and competency (Sommer, 2011, pp. 100–101). While other examples have included more recent events with implementation of ISO 17025 and debates around its success and challenges (Beardmore, Fellows and Sommer, 2017, pp. 38–45). Suggesting that while an authoritative body may be required to regulate digital forensics education such an entity may cause larger debates and potentially weaken implementation dependent on the agency or organisation involved.

Furthermore, Sommer (2011, p. 104) notes that "[c]ertifications, accreditations and registration, qualifications" are usually non-representational of the deliverables they usually relate to; including reason such as:

- loss of sight of the deliverables;
- loss of sight of the delivery value;
- weighted towards recruiting the most applicants;
- weighted towards reducing the costs involved;
- weighted towards a particular product or company.

In these cases, the focus is shaped by, as Sommer puts it, the "economic rule" that, "the more complex and ...[thorough] the assessment process the higher the cost; the higher the cost the fewer the applicants" (Sommer, 2011, p. 103). This attitude can have great impact on the programmes and the worth and quality of the applicants' reward. Multiple authors have made the observation that an accreditation body or scheme could be beneficial to the domain, however also detecting arguments supporting and refuting the ideas (Shakamuri, 2006; Sommer, 2011). Shakamuri (2006, p. 4) takes a more nitty-gritty approach to opinionating subjective views of available certifications; furthermore, acknowledging limitations of the programmes. With the continuous growth of the discipline, also comes what should be the continuous development of important and related training programmes, wise of flexibility for not only trainers but also content (Shakamuri, 2006, p. 6).

It is also prominent that any training course or "strategy should ...cater for the different levels of knowledge and skills needed by ... staff tasked with investigating crimes involving technology" (Council of Europe, 2014, p. 9). The report diagrams the knowledge levels expected against the level and learning requirements of roles in a hierarchical format (Council of Europe, 2014, p. 10), identifying the core skills to be incorporated at a base level. Further, breaking down each role into more in-depth skill-sets on a generic and country basis (Council of Europe, 2014, pp. 9–14). The documentation identifies that the countries involved in the Budapest Convention (Council of Europe, 2001; Clough, 2014) have developed training strategies, however find that the training is "almost exclusively restricted to product vendor training" with very little development or relations made with academic or industry for professional qualifications – "an ad hoc nature [which] ...is not sustainable" (Council of Europe, 2014).

While some literature in this section is starting to show its age, it facilitates understanding where digital forensics education has faced struggles in the past during curriculum design, development, and delivery. This study identifies that these findings and observations must be explored further, particularly in the context of current digital forensics education offerings to identify their validity and relevance. While the observations refer to issues dated back approximately ten to fifteen years ago, their relevance is paramount to the plausible and subsequent challenges which the discipline may have faced and to understand what challenges education may still face today. To achieve this and identify if these are valid observations today, the experiences and beliefs of various stakeholders in digital forensics must be collected and analysed. The relevance of these issues in today's education will be explored, and, at the time of writing, a lack of widely accepted curriculum standards was still an issue.

3.2.2 Background to attempting to deliver frameworks in Digital Forensics

A framework, in its simplest form, is described as a structure designed to support a system or schema and act as a provisional design (Oxford University Press, 2011). For example, a skeletal outline serving as a guide which focuses beyond a single element and looks at how and why things should work based on experiences or designs. A curriculum framework is not principally a curriculum outlined or a stringent mechanism or guide, it is a set of what are predominantly flexible "parameters, directions and standards for curriculum policy and practice" (International Bureau of Education, 2017, p.6). Traditional curriculum frameworks outline content items, often inclusive of knowledge, attributes and tasks, describing the core elements for effective teaching and course structure.

To create a suitable framework or set of standards there are described to be six main steps to consider (Figure 3.1). The development of a framework takes careful thought, experience and time, as well as several stakeholders and for frameworks, standards or certifications to be held with high regard there are several aspects which must be considered such as, the syllabus, competency of trainers and educators and assessment. It is important that the documentation and process of development and delivery are carefully planned, targeted, supported, informed and executed (International Bureau of Education, 2017, p.9).

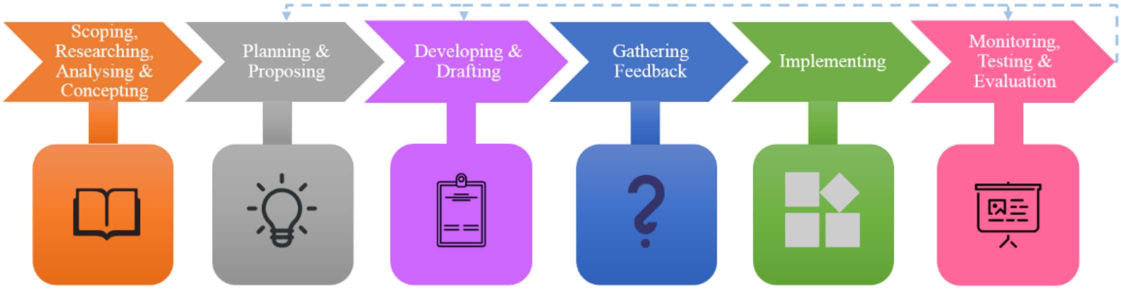

Scoping, Researching, Analysing & Concepting
Planning & Proposing
Developing & Drafting
Gathering Feedback
Implementing
Monitoring, Testing & Evaluation

Figure 3.1 – Steps toward Developing a Framework (International Bureau of Education, 2017, p.9)

Until recent years[9], there has been very little consensus, on the curriculum, nor a framework, for digital forensics and cyber security particularly in professional domains such as policing. Several standards used as an attempt to frame such distinct topics have included the Skills for Justice: Policing Professional Framework (PPF)[10] (Skills for Justice, 2010a), now newly reformed in 2018, which was used to outline the skills, both soft and technical, each policing professional requires. The PPF has been superseded by Professional Profiles (College of Policing, 2018a, 2018d) to describe generic roles across policing and the Competency and Values Framework (CVF) which supports these professional profiles having six competencies in three groups targeting levels of behavioural practice well-rounded by four values (values: impartiality, integrity, public service and transparency) (College of Policing, 2016, p. 3). Behavioural characteristics and competencies range from emotional abilities through to an analytical mindset. These both consider values, education, qualifications, skills and competencies as well as experiences required in these roles. The newest revisions are set to including professional profiles for digital forensics, cyber professionals and are currently trialling profiles for digital media investigators[11]. These draft profiles highlight how an individual must possess sound knowledge in investigative procedures, legislation and boundaries, giving evidence (e.g. in court) and staying abreast with the "changing landscape" of technology, legislation and techniques used to gather evidence. Individuals within these roles are designed to work in tandem with other officers and analyst roles in units such as, Digital Forensic Units, SPoC Units and

[9] Works were delivered after this study commenced.

[10] See Appendix F – F.5 for example work profiles created during the time of the PPF in the UK.

[11] Digital Media Investigators provide assistance and advice when investigations involve digital devices.

Intelligence Units. For example, they must demonstrate education and experience in digital forensics (both computer and mobile technologies), network investigations and open source investigations among other priorities (College of Policing, 2018c, 2018b). While drafts have not been devised, as of yet, for analysts in such units these recent efforts are still unable to provide a framework of requirements.

Other frameworks such as, forensic science curriculum frameworks have attempted to provide general guidelines for programs where some initial details exist on digital forensic topics. Forensic Science saw similar developments when, what was stated as, "huge growth" in the discipline in higher education became an enforcer for quality controls through "the development of its accreditation programme for university forensic science courses" (The Science and Technology Committee, 2005, p. 45). Efforts to transform the digital forensics discipline into a well-rounded and validated topic have also been seen, for instance, by the Forensic Science Regulator: Method Validation in Digital Forensics (The Forensic Science Regulator, 2016).

In most recent years, there has been added focus on cyber security due to government investments and push for an educated workforce in effort to tackle the rising demands for professionals with cyber security skillsets amidst crimes in the cyber realm. Where the UK Government states "cyber risk must be properly managed at the highest levels … the importance of addressing the shortage in specialist skills and deep expertise [where] the Government [were urged] to prioritise its cyber security skills strategy" (Joint Committee on the National Security Strategy, 2018, p. 3).

To this day, the standards surrounding cyber security education are presented at the forefront of curricula design for cyber security and digital forensics in HE. This may arguably be as a result of European and national initiatives such as, the EU's Cybersecurity Strategy (which accompanies the Network and Information Security (NIS) Directive) and the UK National Cyber Security Strategy which look at "principles of cybersecurity" and "achieving cyber resilience" (European Commission, 2013). European strategies clarify that "[e]ach member state shall adopt a national strategy on the security of network and information systems" (European Commission, 2016, chap. II). The directive stresses that strategies must address the issue of "education, awareness-raising and training programmes relating to the national strategy of network and information systems" (European Commission, 2016, chap. II).

3.2.3 Attempts towards accepted standards in HE digital forensics

During the development of this study, several standards for cyber security education which include digital forensics have been implemented. These are outcomes of national cyber security strategies; for example, an updated UK National Cyber Security Strategy for 2016-2021, identifies that "[t]he UK requires more talented and qualified cyber security professionals" where Government initiatives are set to help "supply … the best possible home-grown cyber security talent"; initiatives include cooperation and coordination among stakeholders such as "government, industry, education providers and academia" alike (Cabinet Office, 2016, p. 59). The goals to tackle cybercrimes and to help shape education within this discipline should be considered a positive.

Frameworks today include examples such as, US NIST NICE Cybersecurity Workforce Framework (NCWF) and UK GHCQ certifications (Newhouse *et al.*, 2017; NCSC, 2019) to name but a few. Which incorporate digital forensics as a specialism, topic or work role under the bracket of cyber security; again, adding to the debate and questionably undefined position of digital forensics, a thread within this literature review. Much of the cyber security curricula guidance is, at the time of writing, very new with many works released in mid-late 2017. While not an exhaustive list, Figure 3.2 (below) portrays several frameworks which exist at the time of writing.

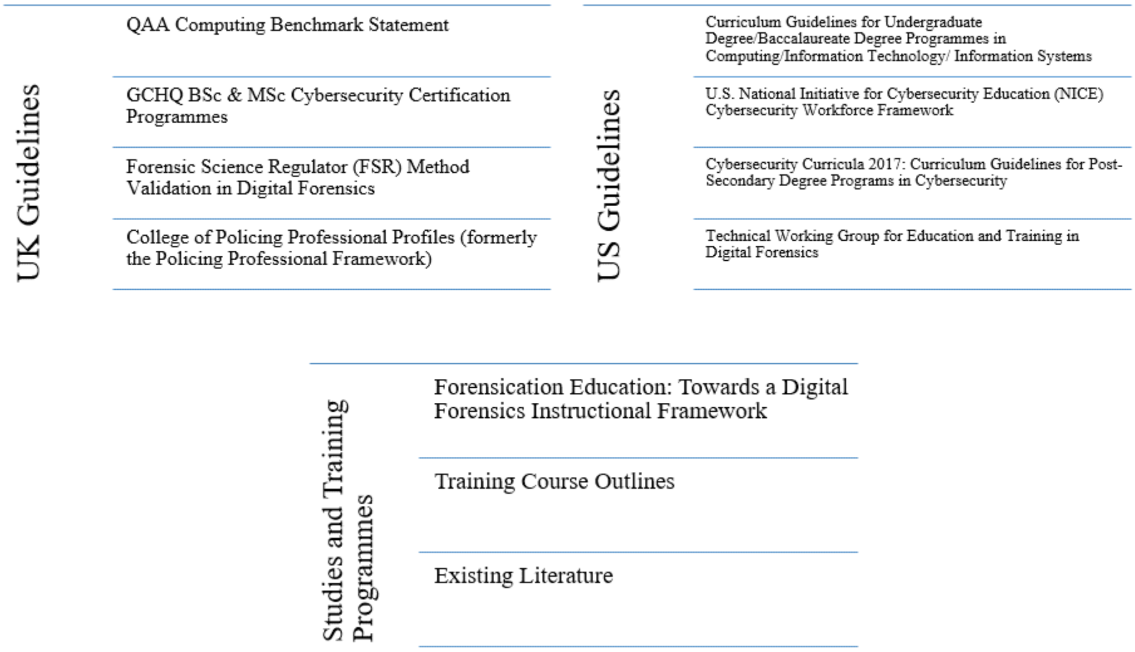

UK Guidelines
QAA Computing Benchmark Statement
GCHQ BSc & MSc Cybersecurity Certification Programmes
Forensic Science Regulator (FSR) Method Validation in Digital Forensics
College of Policing Professional Profiles (formerly the Policing Professional Framework)
US Guidelines
Curriculum Guidelines for Undergraduate Degree/Baccalaureate Degree Programmes in Computing/Information Technology/ Information Systems
U.S. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework
Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity
Technical Working Group for Education and Training in Digital Forensics
Studies and Training Programmes
Forensication Education: Towards a Digital Forensics Instructional Framework
Training Course Outlines
Existing Literature

Figure 3.2 – Frameworks Associated with Digital Forensics Curricula

A commonality among these frameworks are the way in which they are broken down, often into specialist areas or disciplines, most highlighting topics and units which should be inclusive of undergraduate courses. Figure 3.3 (below) further outlines the relationships of key frameworks today and how they break down content and expected requirements.

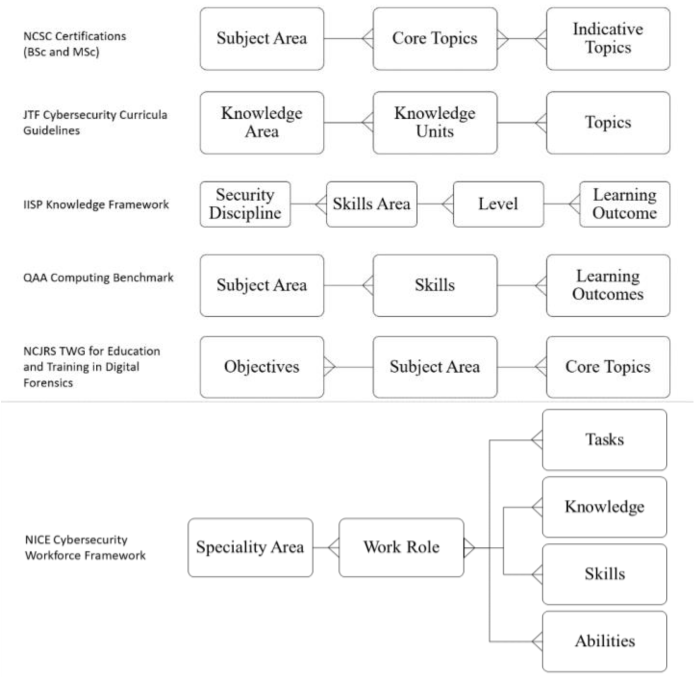


Figure 3.3 – Mapping of Frameworks for Digital Forensics/Cyber Security Curricula

This section considers the following frameworks for their links to digital forensics[12] while identifying their main aims:

- NCSC – Cyber Security, Computer Science and Digital Forensics Certification of Bachelor's and Master's Level UK Higher Education
    - certification states the initiative should:
        - help universities attract additional numbers and higher quality students and help prospective students navigate a range of degree programmes to make more informed choices (NCSC, 2017a, p. 3, 2017b, p. 3);
        - help enhance the quality and focus of degree programmes on relevant aspects of digital forensics and cyber security (NCSC, 2017a, p. 3, 2017b, p. 3); and
        - provide guidance and clarity for potential employers on the content and quality of degree programmes and recognition for graduate capabilities (NCSC, 2017a, p. 3, 2017b, p. 3).
- ACM – Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity
    - curricular guidance states the initiative should:
        - help identify proficiency in cyber security and define a structure for the discipline, identifying a curriculum which is comprehensive and inclusive of industry needs (Joint Committee on the National Security Strategy, 2018, p. 11);

[12] Please refer to Appendix F for detailed breakdown of these standards and frameworks.

        - bring together multiple stakeholders within cyber security to deliver flexible curriculum guidance delivering fundamental principles of the discipline while allowing for change and evolution (Joint Committee on the National Security Strategy, 2018, p. 11).
- NIST – US National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework
    - guidelines to describe cyber security roles:
        - help identify and communicate relevant cyber security roles and the needs of professionals in these positions to support and improve industry, training and education requirements (Newhouse *et al.*, 2017, p. 2).
- E.C.T.E.G., EC3, CEPOL and Eurojust – Cybercrime Training Governance Model – Cybercrime Training Competency Framework
    - work profiles addressing cybercrime roles in law enforcement:
        - help identify and list skills and competences of law enforcement roles relating to cybercrime to help deliver relevant training and certification process materials (Vandermeer, no date).

Among these frameworks there are vast differences in the level of detail provided to breakdown Knowledge, Skills and Abilities (KSAs), tasks, topics and specialisms. For example, guidelines by NIST, the NICE Cybersecurity Workforce Framework (Newhouse *et al.*, 2017), place interest on defining hundreds of explicit tasks, skills and abilities individuals should possess upon completion of their studies. While documentation such as the QAA Computing Benchmark (The Quality Assurance Agency for Higher Education, 2016) omit this level of description and focus on a general understanding of topics required within computing. Furthermore, NCSC standards highlight specific topics which must be covered by either Bachelor's or Master's level courses, with much less details on specific tasks and skills. Some may argue that this provides flexibility for courses from a range of backgrounds to meet criteria among specifications and certification.

Most, if not all, frameworks also provide key learning objectives and/or outcomes for a programme of study; something current HEI course documents provide where specifications outline course aims, goals and objectives broadly allowing for flexibility in course delivery. For most UK institutions offering a course in digital forensics and cyber security, focus is still placed on the QAA Computing Subject Benchmarks and QAA Codes of Practice as reference in programme documentation, at the time of writing. Works such as those by the UK's NCSC (2019) are slowly becoming a point of reference for more institutions with provisional or full accreditation. Due to fresh implementation of these standards, outcomes and benefits of such accreditations cannot be examined, however, this review considers the detail of several standards and frameworks.

While the level of detail each documentation offers differ, open coding at a very broad level within this review shows that there are several keywords and topics which are dominant for digital forensics, based on the first three frameworks (portrayed in Figure 3.4). A review in chapter 2 highlighted that from module naming conventions it was not always possible to identify topics and content learned by students on a degree programme. However, frameworks and standards such as those examined in this section go some way in helping identify what is required and whether courses, if certified, are meeting such criteria.

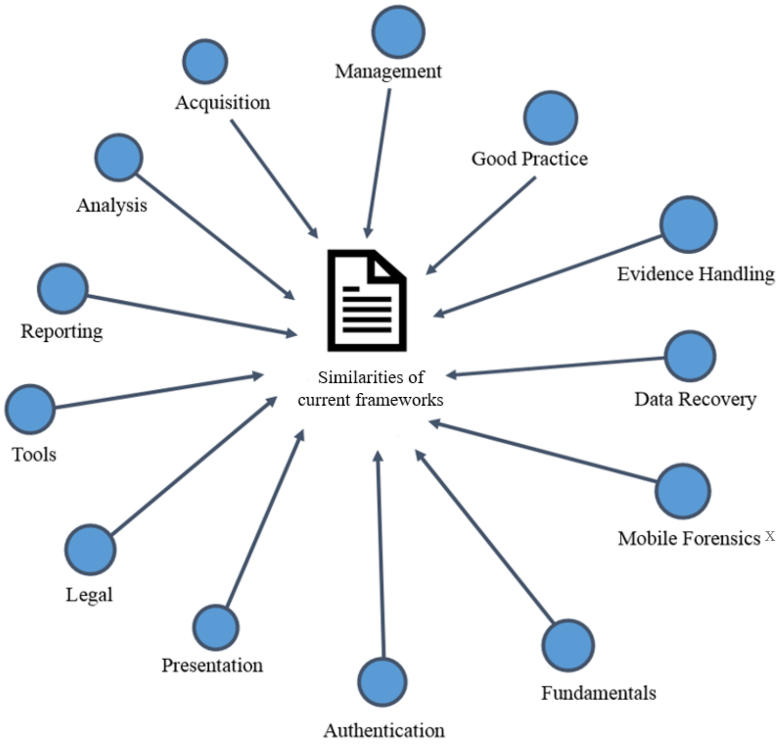


Figure 3.4 – Coded themes for digital forensics within current cyber security frameworks

These themes are supported by work conducted by Dafoulas, Neilson and Hara (2017, p. 149) who state that digital forensic courses should focus on five themes in order to synchronise programmes and underpin the discipline. These are depicted in this thesis as the Five-K's in Table 3.2, below. While these efforts show some standardisation and attempts to synchronise programmes, particularly in the UK and US, there may be concerns toward certifying degree programmes and identifying how these standards have been accomplished. For example, there are a relatively small number of courses in the UK who have a) put their course forward for certification or b) gained certification for digital forensic courses both at Master's and Bachelor's level via the NCSC; most are seen in cyber security (NCSC, 2018b).

Five-K's	Knowledge	Examples
Themes		
K1	Stages of an Investigation	“Seizure, Acquisition, Preservation, Analysis and Reporting”
K2	Investigative Skills	“Handling of Evidence and Professional Practices”
K3	Professional Practices	“Practices which form the foundations of Computer Forensics”
K4	Criminal Justice, Legislation and Regulations	“English Legal System, Legislation and Processes, Regulations and Standards related to Digital Evidence and Forensics Investigations”
K5	Computer Fundamentals	For example, “Data Storage, Operating Systems, File Systems and Computer Networks”

— (taken from Dafoulas, Neilson and Hara, 2017, p. 149)

Table 3.2 – FORC[13] Project Analysis Five-K’s

There may arguably be reluctance to put courses forward for this certification if they require too much change or there appears to be little or no expected benefits from this process. Though, the NCSC promote the degree certification by expressing that the uptake of HEIs offering cyber security degrees “can be difficult for students and employers alike to assess the quality on offer and to identify the degree that best suits someone’s preferred career path” (NCSC, 2018b). Champagne (2015, p. 18), writes:

> “Sound policy that defines expectations does not substitute for quality forensic practitioners and technical process. Rather, it should be considered as a complement to them and a guide that will help an agency navigate the scientific world of digital forensics.”

Relating Champagne's (2015, p. 18) thoughts on policy and expectations to the addition of frameworks attempting to define, standardise and provide curriculum coherence of educational programmes, the works should as mentioned provide guiding principles which should complement the educational system and industry alike to assist with the production of quality and effective, be it initial, practitioners. Frameworks should highlight and continuously revise the knowhow expected of e.g., degree students, based upon technological and industry changes and enhance while providing guidance to navigate the digital forensic and cyber security curricula. This identifies that there is a need to acknowledge experiences and views of multiple stakeholders involved within the process of digital forensics (ranging from academics, industry

[13] An EU funded pathway in Forensic Computing (FORC) project

professionals through to graduates and students themselves) to identify the successes of education for digital forensics: a key aim of this thesis and something captured in later chapters.

Similar initiatives to educational frameworks include European collaborations within law enforcement such as, the development of the Cybercrime Training Competency Framework by the European Cybercrime Centre (EC3), and other bodies (Sobusiak-Fischanaller and Vandermeer, no date; Nogala *et al.*, 2016, p. 18; Vandermeer, 2018) which work towards delivering competencies deliverable of professionals in the cybercrime roles. The work includes digital forensics in a time when it is recognised that there is a "need for training and continuous learning" as well as "proactive sharing of best practices and innovative tactics" (Wainwright, 2016, p. 15). Section F.4 in Appendix F highlights the roles relating to digital forensics and the necessary expert and basic knowledge required. However, this information is broad such as, the need for "digital forensic skills" (Sobusiak-Fischanaller and Vandermeer, no date; Vandermeer, 2018). While no specific attributes, skillsets or tasks similar to the NIST framework (Newhouse *et al.*, 2017) are mentioned, the E.C.T.E.G. training materials and course outline identify specific knowledge areas which can be used as a comparison to educational frameworks discussed above (European Cybercrime Training and Education Group, 2019). For example, E.C.T.E.G. course outlines show available training materials relating to areas such as:

- forensic scripting (python) and Linux as an investigative tool;
- specific operating/file system forensics (e.g. Windows/NTFS/Mac/mobile/data storage);
- live data forensics;
- network forensics;
- malware analysis;
- databases and data mining;
- the Darkweb and virtual currencies; and,
- open source/Internet investigations.

— (European Cybercrime Training and Education Group, 2019)

Topics highlighted of these courses show similarities with educational frameworks such as the need for programming and scripting, network forensics, OSes and files systems and databases. However, these courses also highlight topics including open source investigations as well as the Darkweb and virtual currencies which are rarely mentioned in educational frameworks and an omission in course descriptions and module naming conventions for UK HE degree programmes.

3.3 Research Gaps

Referring to the research questions described in section 1.1, Figure 3.5 highlights the research gaps this study looks to address, while taking into consideration the problem statement and literature analysed. These gaps are determined based upon the review and investigation conducted throughout chapters 2 and 3.

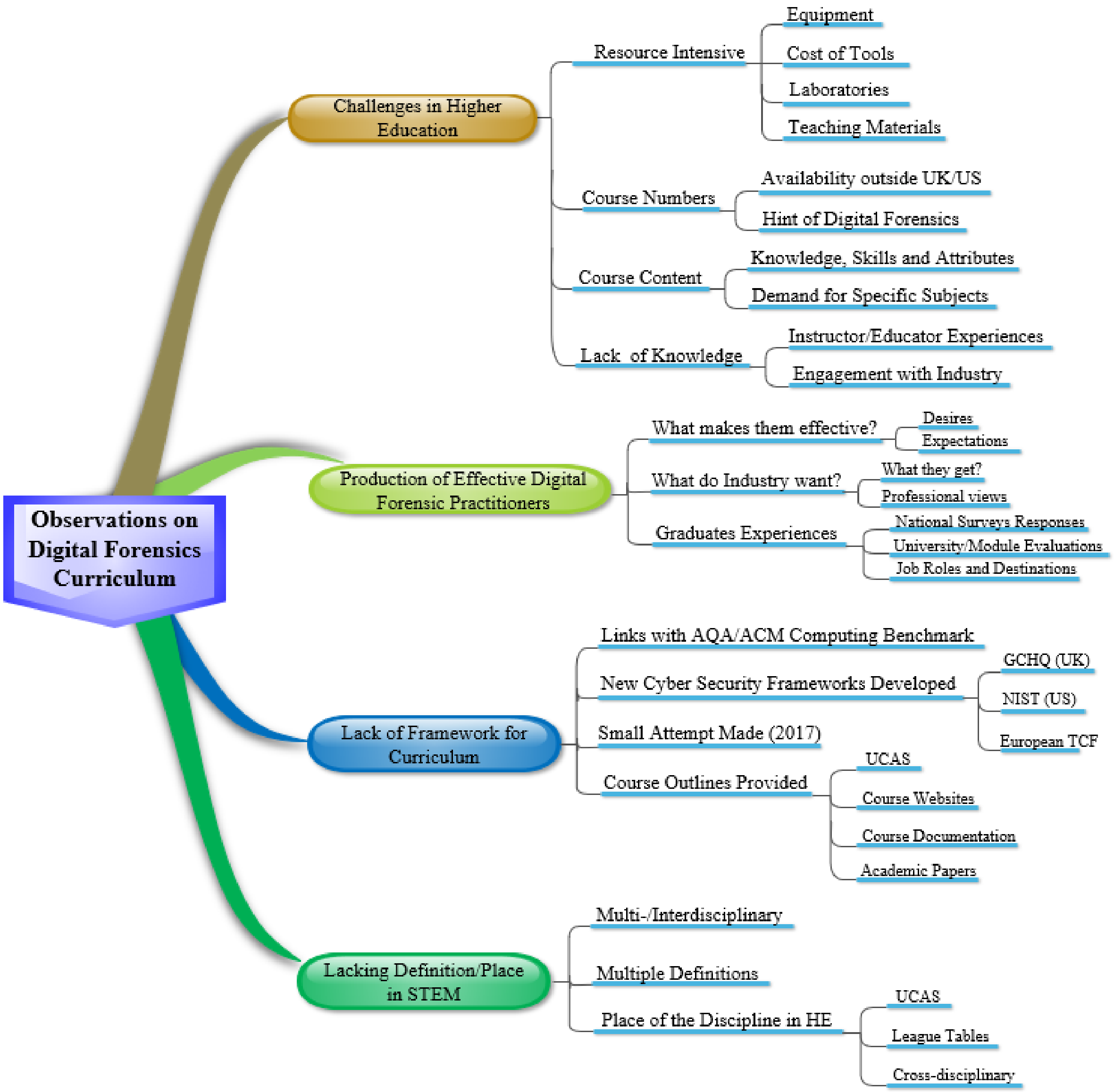

Observations on Digital Forensics Curriculum
Challenges in Higher Education
Resource Intensive
Equipment
Cost of Tools
Laboratories
Teaching Materials
Course Numbers
Availability outside UK/US
Hint of Digital Forensics
Course Content
Knowledge, Skills and Attributes
Demand for Specific Subjects
Lack of Knowledge
Instructor/Educator Experiences
Engagement with Industry
Production of Effective Digital Forensic Practitioners
What makes them effective?
Desires
Expectations
What do Industry want?
What they get?
Professional views
Graduates Experiences
National Surveys Responses
University/Module Evaluations
Job Roles and Destinations
Lack of Framework for Curriculum
Links with AQA/ACM Computing Benchmark
New Cyber Security Frameworks Developed
GCHQ (UK)
NIST (US)
European TCF
Small Attempt Made (2017)
Course Outlines Provided
UCAS
Course Websites
Course Documentation
Academic Papers
Lacking Definition/Place in STEM
Multi-/Interdisciplinary
Multiple Definitions
Place of the Discipline in HE
UCAS
League Tables
Cross-disciplinary

Figure 3.5 – Gaps Identified in Research

3.4 Summary

While chapter 2 focused on the review of current literature surrounding the delivery and current position of digital forensics within higher education through academic programmes and academic research, this chapter considered the most recent works of standards and frameworks from national bodies where a shift towards cyber security has been seen. Analysis of these standards have to some degree considered the questions: *what is expected of an individual with a degree in digital forensics?*, and *what are current standards and frameworks and how are they applied?* Both are important toward answering the most pertinent question: *what makes an effective digital forensics practitioner?*

Review of these standards has shown that there are particular areas which a programme must focus on and enable students to appreciate and contextualise, ranging from: investigative skills and knowledge through to more specific learnings such as, Operating System Forensics including mobile devices and legal and regulatory processes and issues. Comparable to findings in chapter 2, where it was shown to be difficult to identify the inclusion of these areas, these standards show that there are vast quantities of information which a student studying digital forensics must learn technically and theoretically.

Each standard introduced mid-end way through delivery of this study have identified key topics and specialisms, some even identifying specific attributes (e.g., knowledge, skills, abilities and tasks) however, their uptake within education is still relatively new with little identification toward their benefits to the educational system and digital forensics industry. Though, these specialist topics and attributes can be used to reflect and compare with the views and experiences of various stakeholders, particularly professionals who may have found shortcomings of the graduates within industry or graduates who have been able to identify shortcomings of their studies.

While standards have been developed by groups of professionals (industry and academic), this review finds there is still the need to capture views from a range of audiences (including graduates and students) to obtain their experiences, views and ideals: a narrative which is missing in the current literature and a gap this study aims to fill.

To accomplish this, the views and experiences of individuals who have experiences of education and/or training in digital forensics, and those who educate and/or work within the field of digital forensics and, by extension cyber security, is essential. This research progresses by capturing people’s experiences to give voice to a range of stakeholder groups within the education of digital forensics and discover known challenges, positives, and skills-shortages within the field, and how education may better facilitate in closing the gap. This research identifies that there are key several stakeholder groups to consider within education such as, academics, students, graduates, professionals, and extends to the public for purposes of rigour. To capture people’s thoughts, opinions, experiences, and ideals, this research will utilise qualitative methods as these are best suited to social settings and phenomena such as experiences. These methods are discussed and explained in chapter 4.

4. METHODOLOGY

INTRODUCTION

This chapter discusses the fundamentals of the overall research design for this study, making clear connection between the research problem/questions and its goals using the methods outlined for collecting and analysing data. There are five parts to this methodology; the first focuses on the overarching research questions and goals, addressing the research problem and assumptions which underpin the study. The second looks to positioning the researcher; identifying their background and experiences and how or why these may influence, or provide limitations to, the research. The third part efforts to highlight more of the 'how's and 'why's' of this research, looking at why this research takes a qualitative approach and how considering methodologies adopted. The fourth component centres on the intrinsic elements of research design, for example: the methods used to collect and analyse data. This part considers the limitations of the chosen methods and in areas such as, identifying the selection of participants and gaining access. The final part looks at the overall limitations of the methodological approach and considers differing approaches and methods which could have been adopted and justifications for non-application.

4.1 Direction of this Research

Reviews conducted in chapter 2 and 3 have served to inform and confirm the direction of this research. Chapters 2 and 3 have highlighted how the field of digital forensics has struggled with debates over standardisation and certification, training and education, resources and staffing and overall the dependency on digital technologies and their continued advancements. Similarly educational institutions offering digital forensics over the last decade have faced similar challenges with offering relevant, realistic, and valuable programs. Chapter 2 highlighted the key topics that are present in undergraduate offerings in the UK and highlighted the issues with the delivery of course information, for example, the brief and short descriptors, generic titles and more. All affecting the way a course is demonstrated, and the understanding of what may or may not be included in a course. Arguably the review of these materials have also shown that courses seem to continue to adopt a computer rather than digital forensics approach, with more and more courses focusing on cyber security with an element of digital forensics.

Chapter 3 also looked at how there is a lack of widely accepted standards in digital forensics not only in the field, but in education too. This affects who determines what is effective and how an educational course or individual who has experienced a course can be determined as being effective for industry. While standards were slowly introduced toward the end of this study, the efficacy of these standards and their application to educations has not been explored.

Considering the observations and findings in chapter 2 and 3 these have confirmed the direction of the research, namely, focusing on the current state of the UK education in digital forensics at undergraduate level due to the plethora of courses available, and looking to what makes an effective practitioner. Little works so far have explored these questions, some have outlined course development and delivery, as well as the learning concepts applied in digital forensics which have seen placement on problem-based learning and have been recently seeing a shift to gamification, however, the overall effectiveness of graduates produced is not considered. Challenges with learning, implementation and the wider community were explored with anecdotal examples in literature from the experience of academics writing the papers. Or, from professionals involved in surveys about current challenges faced in the field. However, in-depth experiences and opinions are rarely explored. Thus chapters 2 and 3 highlighted how there are few works concerned with the opinions and experiences of several stakeholders combined, critiqued, and compared within digital forensics.

This research therefore identifies that the narratives of serval stakeholders within digital forensics must be explored to assess digital forensics education in the UK and its outputs e.g., graduates for industry. These stakeholder experiences, views, ideals, and beliefs are to be explored in this research to address original research questions which focused on:

- the current state of digital/computer forensics education (e.g. topics, challenges, and recommendations)
- the developments towards curriculum frameworks reflective of industry needs, and
- effective practitioners and/or curriculum (e.g. knowledge, skills, learning and practice).

Such experiences, opinions, ideals, and beliefs across five stakeholder groups (academics, students, graduates, professionals, and the public) will be considered using a qualitative approach to digital forensics education. This methodology highlights the use of interviews, questionnaires, and workshops to achieve these results, and until now these methods or stakeholder groups have not been explored collectively.

4.2 Positioning of the Researcher

Creswell and Poth (2016) note that the researcher needs to consider their own "biases, values, and experiences that he or she brings to a qualitative research study". The researcher is an instrument within qualitative research and is paramount to the research process through the collection of data, data analysis and write-up. Therefore, the researcher has influence at every stage.

Taking data collection as an example, the researcher has influence in devising questions for the overall research as well as influencing respondents when interviewing and questioning (e.g. through leading questions or elements of own bias). Further considerations toward behavioural observations and instructions, examination of documents and the observation of social settings are also required. The data analysis stage may also be influenced by the researcher. The researcher collates and analyses data from multiple sources of information and reviews categories and themes across and among them, building several patterns with a level of subjectivity and personal interest.

Qualitative studies, often where one individual is the sole driver of the study, will include an element of researcher subjectivity. Although, it can be argued that, the position of a researcher is not biased unless they fail to acknowledge the part they play and the consequences and impacts they may have upon the research and its participants. The researcher must be reflective of their position and try to enforce some objectivity. Creswell (2014, p. 186) discusses reflexivity noting that the researcher must be aware of their own experiences and their "potential for shaping their interpretations, such as the themes they advance and the meaning they ascribe to the data" where an open and honest account of the researchers' background, history and even gender can be an influence.

Creswell and Poth (2016) identify two parts of reflexivity that the researcher must consider: their experiences with what is being explored and how these experiences impact the researcher's understanding and analysis. These are considered in Table 4.1.

Reflexivity	Position of the Researcher	Addressing the Researcher's Position
Researchers experience with the topic	→ Academic Role in Computing and Digital Forensics → Researcher in Digital Forensics Education	→ Considering the researchers own knowledge and discovery of the topic → Identifying own thoughts on the topic and their influential power (to the research and the respondents)
The impact of the researchers past experiences	→ Forensic Computing Alumnus → Route into Academic Role in Computing and Digital Forensics	→ Considering and announcing own learning biases and educational experiences → Considering and discussing own experiences within academia (as a student, graduate, and staff) → Noting and highlighting the experience and limitations of the researchers - own teaching knowledge and experience - own professional experience and knowledge

Table 4.1 – Considerations for the Researchers Position and Reflexivity

Throughout this research the researchers own bias and reflexivity is considered by addressing their background and preconceptions, as discussed in section 4.2.1.

4.2.1 The Researcher's Background

The researcher's background developed from a strong curiosity in computing; where, further passion developed in to teaching. The avenue the researcher took diverted into an interest in understanding the criminality behind technological use and how the devices are investigated to aid criminal justice. This led to the researcher undertaking an undergraduate education in forensic computing; with a passion to teach still brewing.

During the researcher's time studying at undergraduate level they noticed there was this growing demand for practitioners recognised due to technological advances and growth in digital crimes. Yet, there was little research which focused on the effective digital forensic practitioner from a range of insider perspectives (e.g. students, graduates, professionals, and academics). The researcher's interests were drawn to the following observations which captivated the need to question what makes an effective practitioner within the discipline:

- the growth in programmes provided at UK Universities offering digital forensics, however, no identification of their nature, progression or stand out values;

- a cloud was suspended over the subject due to struggles in, and the expense of, resourcing such a degree (ranging from hard and software struggles and their monetary expense through to the creation of real-life scenarios for educating and assessing); and
- no real consensus on frameworks to adopt when teaching or training within digital forensics (much of the literature discussed the organisation of programmes or learning styles adopted to facilitate such technical knowledge).

Since studying a degree in Forensic Computing at Canterbury Christ Church University, the researcher has subsequently had the fortune to enter into the academic arena: studying, training and teaching. The researcher has served as a University Instructor in Computing from October 2014. This experience has provided the researcher with the opportunity to confront many of the challenges previously outlined within the literature and has provided a wealth of understanding.

As described by Coe *et al.* (2017, p. 188) evaluation of the researcher's own bias is more crucial "than to pretend they can be nullified" and entirely repressed where the researcher can "use their prior knowledge and experience to good advantage". The researcher believes that their academic role and previous studies in understanding and experiencing digital forensics within higher education enhances awareness, knowledge and curiosity toward the problem statement of this research. Subsequently, the researcher's views and interpretations will have been shaped by their own experiences. It is here that the researcher must consider a certain level of bias this can add to the study, where efforts are placed on minimising these to ensure objectivity. Efforts included consistent and neutral data collection methods where the researcher refrains from revealing own opinions and preferences.

Let us take three examples where the researchers own opinions and experiences must be considered as an influencer and efforts to ensure objectivity must delivered:

- the experience the researcher has with observing students at their own institution; this can exhibit preconceptions on the overall student experience while also the potential to effect perceptions of such teaching elsewhere;
- the researcher's own educational experiences and encounters may influence the direction of the study and interpretations of others' views, beliefs and experiences;
- the researcher's own experiences in delivering curriculum in a digital forensic degree and training; this can affect the questions posed to others and their opinions and views.

We must also consider the influence of the participants own experiences on their responses and in turn the interpretations the researcher can make. In cases where interviews and observations took place, the background of the participants were identified to help the researcher construe views, beliefs and encounters.

Let us take an example of a fabricated professional participant (depicted in the box below). For this practitioner their on-the-job experiences led them to the opinion that experience is more important. Many influencing factors to their response were for example, their route into their work role and length of experience, their lack of educational experiences and tendency to undergo training as well as the case experience they would embark on.

Fabricated Example - A question is asked about the value of experience, education and training to a practitioner who a former police officer now working in a role within a Digital Forensics Unit (DFU) with ten years' experience. The police officer has no educational experience but has worked their way through their roles by on-the-job training and through experienced gained. The practitioner believes that experience and training are more important than educational qualifications. That the crucial understanding and know-hows of the job are best sought through practice and hands-on encounters which outweigh theoretically based educational settings. Thus, for them the influence of their experience may lead them to answering yes, experience is more important.

This example highlights the need of the researcher to form a rapport with individuals, gauge an understanding of the previous practices and happenings of the participants to inform their own interpretations and the extent to which the viewpoints are contemplated and regarded.

On the other hand, within this research, the researcher must consider the negative influence a participant may have in accordance with a participants tendency to provide what is described as a "socially acceptable answer" (Lavrakas, 2008, p. 375). Social desirability bias can often be seen in interviewing and questionnaires/surveying techniques and, in general, the presence of an investigator (i.e. the researcher) can increase this effect (Groves *et al.*, 2009, p. 170). It is the notion of the interviewee agreeing with the interviewer, or the agreement with statements in questionnaires to provide what they (the respondent) believes to be an acceptable or correct answer. The underlying conviction for performing social desirability is so to "portray themselves or an organization … in a favourable light" (Lavrakas, 2008, p. 429). This may result in responses which reflect an agreement with the researcher and thus do not shed light on the participants views resulting in an inaccurate measure of the research interests.

The methodical approach of this research was guided by the lack of analysis of the qualitative and narrative style in the domain for experiences in teaching and learning digital forensics from several audiences. Much of the forerunning academic literature focused on the qualitative side of developing a digital forensic programme and the topic as a fundamental discipline. These works however drew to attention the lack of voices and accounts (e.g. views and experiences) of multiple stakeholders in the delivery of digital forensics investigation and education. Particularly, academic pieces which have focused on program delivery have omitted these voices and have evaded the qualitative analysis of whether effective practitioners are produced in both education and training in the view of the very profession they seek employment. These questions and curiosities guided the methodological approach, seeking to identify the voices and accounts through interviews, questionnaires and observations to pull together qualitative pieces. With the main overarching objective and question to analyse what makes an efficacious practitioner.

4.2.2 Lenses, Paradigms and Limitations

There are several ways in which interviews are treated as a resource in research, however, the researcher must consider how these methods are oppressed with judgements and values of their participant and themselves. The limitations of how the respondents' own experiences, thoughts and beliefs might affect their current responses and opinions e.g., their own subjectivity due to study or careers is also a consideration. Furthermore, within this study there are several lenses utilised; a lens is described in qualitative research as the researcher "using the views of people who conduct, participate in, or read and review a study" (Creswell and Miller, 2000, p.125 cited in Ravitch and Carl, 2015).

To address validity, verification, reliability and credibility within this research techniques such as triangulation (e.g., ensuring rich data through multiple data sources and data collection methods), prolonged engagement (e.g., adequate time spent in a setting, dialogues with many people where relationships and rapport are built) and thick description (i.e., sufficient details to draw themes and evaluations of data collected) are considered.

4.2.2.1 Data Triangulation

This research has been conducted using a combination of approaches, where data triangulation has been useful and comprises of both primary and secondary data. Data triangulation is depicted by Denzin (1970, cited in Flick, 2017) as the use of more than two sources of data within a study to increase the validity. This is also typically the most popular type of data triangulation used within research alongside methodological triangulation (Denscombe, 2014, p. 154). For example, within this research, interviews using the same research techniques are used to obtain data from different participants (academics, graduates and professionals). During the process of data analysis, responses and feedback from the groups are compared to determine areas of agreement and divergence. Data triangulation is particularly well-suited for this research due to the number of target groups identified (five) and their vested interests in digital forensics and/or cyber security education and training. The triangulation of these are of importance and to some degree strengthened by the lack of positioning of the digital forensics discipline. Anecdotally, the disciplines are viewed by many as two distinct and separate subjects, others view these as subsets of each other, these differing views and placements of the subjects bring together the need for triangulation of data within and among the target audiences.

Furthermore, methodological triangulation (Ritchie and Lewis, 2003, p. 276; Flick, 2008, p. 44) of different qualitative methods is utilised to allow for combination of different perspectives across the research questions and phenomenon explored. Where participant numbers are low, methodological triangulation is also used to extend data collected against one particular method. For example, results from both questionnaires and interviews can be compared to literature survey and document analysis to see if similar results are found (Figure 4.1).

There is a large debate among authors about the value of triangulation (Ritchie and Lewis, 2003, p. 46); where, the main disadvantage is the necessity to organise and plan the collection of more data, alongside why triangulation strategies are necessary in the first place within a study (Jick, 1979; Weyers, Strydom and Huisamen, 2014). For example, within this research interviews were designed to be the main focus of data collection and planned from the outset. Where key themes were generated but data saturation had yet to occur the use and availability of questionnaires to obtain further voices were employed. Although, the benefits of triangulation outweigh the negativities in planning and organising for the positive increase in validity and confidence in research data which can be accomplished (Jick, 1979; Weyers, Strydom and Huisamen, 2014). This allows for creative ways of understanding and answering the questions within this research, in effort to further highlight and present new and unique findings among curriculum research within digital forensics.

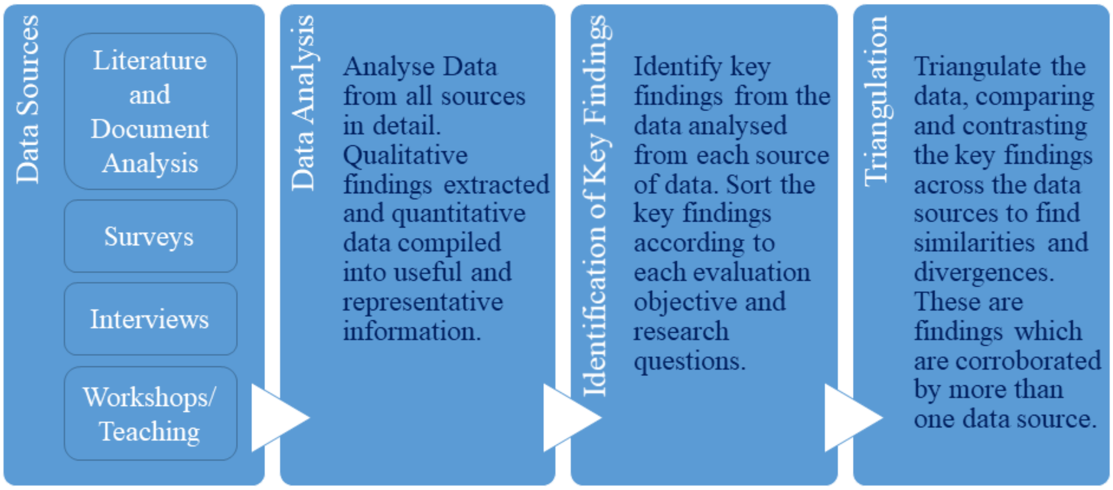

Data Sources
Literature and Document Analysis
Surveys
Interviews
Workshops/ Teaching
Data Analysis
Analyse Data from all sources in detail. Qualitative findings extracted and quantitative data compiled into useful and representative information.
Identification of Key Findings
Identify key findings from the data analysed from each source of data. Sort the key findings according to each evaluation objective and research questions.
Triangulation
Triangulate the data, comparing and contrasting the key findings across the data sources to find similarities and divergences. These are findings which are corroborated by more than one data source.

Figure 4.1 – Triangulation of Data Sources

4.3 Research Context and Strategy

This section highlights how and why the research has been conducted using a combination of practices and focuses on a qualitative approach. To understand further the methodological strategies, data collection methods, and analysis methods used within this research, the gradations of these approaches are discussed below.

4.3.1 Why a Qualitative Approach?

> "The intent of qualitative research is to understand a particular social situation, event, role or group, or interactions."
>
> – (Locke, Spirduso and Silverman (1987, cited in Creswell, 2014, p. 205)

Firstly, both qualitative and quantitative research must be explored. The most exhausted and simple definitions provided are that quantitative research deals with numbers as data and, that qualitative research deals with words as data. With each there are key issues considered when planning, conducting and reporting of information within phases, processes, data collection and data analysis.

Onwuegbuzie and Frels (2016, p. 5) state that "there are three main research traditions": qualitative, quantitative and mixed research. Approaching any study involves critical considerations towards strategies used to obtain and analyse data as well as identifying the focus of research components conducted. Within research, it is contended that there is a selection process for qualitative and quantitative strategies. Some studies embrace a multitude of methods from both (i.e. mixed methods). Creswell and Creswell (2017) discuss how "a study *tends* to be more qualitative than quantitative or vice versa." Largely noted, the difference between qualitative and quantitative is the subjectivity that is produced when conducting qualitative research.

Characteristics of quantitative methods produce data in the form of numbers and logic; methods are objectively used to discover how many, much and often; a measure of understanding and relationships. Observations and measurements are designed to be replicated by others to produce the same results. Quantitative methods also allow for the generalised concepts to investigate these relationships, the ability for future predictions and production of statistical models. Although quantitative methods are useful for numerical and logical data, they are less fruitful in design for behaviours, social responses and deeper social understandings.

Qualitative research, on the other hand, is more aware of society and open to less rigid designs (Atieno, 2009). Studies purposefully look towards the social aspects which are more information rich involving the sampling of people, cultures, demographics, communities and events (Patton, 2002). A multitude of data collection strategies such as observations, interviews and case studies are used within qualitative studies to provide insights into personal and social perspectives, experiences, beliefs and views. With this, the data collected is concerned with verbal descriptions and accounts of experiences where analysis is conducted on textual and audio responses to code and identify themes.

Particularly within education qualitative measures such as interviewing, and observations are particularly advantageous. Due to the nature of qualitative research, to look deeper and beyond the numbers, questions surrounding subjectivity are present.

Considering the objectives of this study i.e. the need to understand the experiences, views and beliefs of a range of participants within the domain of digital forensics education and training, this research does not lend itself to measuring by numbers nor creation of a piece of software or tool. Thus, this research adopts very little quantitative methods. Although, where necessary, quantitative methods are embedded into a qualitative research design to provide a more meaningful embedded interpretation. Contrarywise, a quantitative survey to compare the delivery, resourcing and implementation of courses and their success rates could have been achieved. However, these would have yielded results not descriptive to the research problem and aims for articulated views. Working on the theory that there is a strong sense of subjectivity in what makes an ‘effective practitioner’ and how education and training compare and deliver to achieve this, the need to understand and consider the voice of several respondents became a prevalent understanding.

To fulfil this, it is clear, quantitative methods are not equipped to observe and investigate this socially driven research and the subjectivity of respondents. Although, quantitative approaches can be used in questionnaires to discover, for instance, the resources of different undergraduate programmes and establishments, keeping note that the response rate of such can be extremely low, even when using digital communication methods to spread the research. Due to the social drive of the study, flexibility is required to much greater extent to capture the deeper understandings necessary to discover the knowledge and views of all target groups and compare and thematically analyse. A largely qualitative design therefore has been used to investigate the views and experiences on the specific topic of digital forensics education and training for producing effective practitioners. Methods adopted such as, interviews and questionnaires have been considered with respect of their target group. For example, the methods employed for gathering views of students may differ from those when gathering data from police officers in training.

Onwuegbuzie and Frels (2016, pp. 6–7) outline that qualitative research comprises of several components and highlights the direction and details, and purpose in context, of the research ideas and questions through to data collection methods. Table 4.2 pinpoints four of these components highlighting data collection methods adopted throughout this chapter and its formation.

Element	Qualitative Research
Research Objectives	→ exploring, describing and developing
Research Questions	→ *tend* to be open-ended, non-directional and emergent → *tend* to address the "what" and "how"
Data Collection Methods	→ interviews, observations, focus groups, case studies → action research, literature survey, grounded theory → field notes, documents
Nature of Research	→ natural environment/setting of social phenomena → *tends* to address the way things are → seeks to answer the "why" and "how"

Table 4.2 – Qualitative Research Components

Looking at research aims of this study, it is apparent that the study focuses, and is centred, on the participants where it strives to measure social responses from five main target groups (industry professionals, students, graduates, academics/trainers and the public) with an interest in digital forensics and reaching to cyber security. Information such as opinions, experiences, behaviours, and motivators require a form of rapport with the participants to gain valuable responses. What needs to be considered however are the connections and themes that can exist among the target groups identified (Figure 4.2). These include the previous life-experience of the individuals e.g., were they once a student and now a professional.

For example, a professional considered in this study may also be an alumnus of Canterbury Christ Church University and once a student/learner. This is resembled in the middle of the Venn diagram in Figure 4.2.

The figure also represents the overlaps of, for example, an academic who was once a professional or even potentially an alumnus. The diagram shows strong links between professionals, graduates and students; although this is not to say their views and experiences are similar or in fact different. Nevertheless, the experiences of a professional who is a graduate and was once a student may influence the views and beliefs of that individual more so than for example a professional with on-the-job experience who has become an academic. The social interactions and professionalism obtained can be dramatically divergent and may ultimately influence the expectations and requirements and may reveal themselves in different manners, actions or emotions. The public respondents in this research are not intertwined with any of the other four target groups insomuch as, they may link with new students. This is a subjective bias placed on the study by the researcher whose own experiences in describing the discipline to the public and fresh students is often similar and thus the public respondents fall just short to the left of students within Figure 4.2 to depict the closeness of views and experiences prior to study. This is again subjective in the categorising fresh-faced students with the public, where it could be noted that some students have a deeper understanding of the discipline due to their eagerness in computing, computer science, digital forensics, cyber security or even through their own experiences in earlier education adding yet another level of subjectivity.

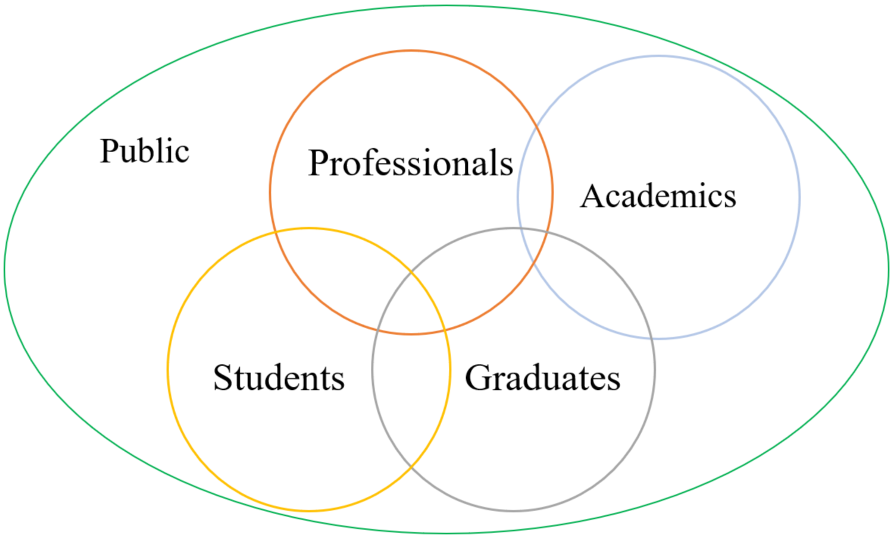


Figure 4.2 – Research Target Groups and Associations

Table 4.3 identifies stages throughout this research, the target group they seek to discuss, and the methods used to collect data and thus evaluate results. It demonstrates that questionnaires and interviews were the key collection methods utilised in this study, and while it may be found that different methods were used for comparable groups, these were selected carefully.

Stage	Target Group	The Research	CH
Data Collection/ Evaluation	Academics	Questionnaire/Interviews	5/6
	Graduates	Interviews	6
	Students	Workshops/Questionnaire	6
	Professionals	Questionnaire/Interviews	7
	The Public	Questionnaire	8

Table 4.3 – The Research Stages in Context of Chapters

This study identifies the need to examine the discipline further using several stakeholder experiences and beliefs; questionnaires and interviews are a beneficial technique due to their qualitative nature and capacity to capture in-depth responses. This research looks to uncover the story behind experiences of digital forensics education and gather in-depth information to explore central themes within education of the discipline. Questionnaires are useful to explore and collect data from a large sample in a standardised way. In this study questionnaires are also used due to their convenience and ability to reach a wider population which suffers from difficulties of access.

A questionnaire was used in chapter 5 to collect information about resourcing issues by academics and allowed for both qualitative and quantitative responses. Chapter 6 explores more responses from the interviews with academics targeting their involvement in the design, development and delivery of educational programmes and their experiences across the years. Chapter 6 also explores the results from student workshops which included a questionnaire of quantitative and qualitative approaches which explore student views and expectations. In addition, Chapter 6 explores in-depth interviews with graduates who recollect their university experience, their learning and application on-the-job. Chapter 7 explores the questionnaires and interviews from professionals, where qualitative experiences and expectations were sought regarding education, training, and topical content. Furthermore, Chapter 8 explores a questionnaire that targets the public looking to identify their understanding and experience of digital crimes.

This section comments particularly on the use of these methods, based on each stakeholder group. While each stakeholder group might otherwise appear comparable, different methods were employed based on several factors, and namely the issues related to gaining access to participants (further discussed in section 4.4.6.3).

4.3.2 The Application of Research Building Blocks to this Research

This section discusses the fundamental research building blocks of any study and concentrates on their application within this research providing assumptions, justifications, and limitations of approaches to this qualitative examination.

4.3.2.1 Literature Survey

A literature survey is an objective and systematic summary and critical analysis of existing and relevant research in the topic area studied; the goal to explore topical information to help justify the research (Onwuegbuzie and Frels, 2016, p. 8). This thesis adopted a literature survey in Chapter Two to provide the audience with a comprehensive background of digital forensics within academia. Furthermore, literature surveys are employed throughout to elicit information regarding multiple aspects of research pertaining to, for example: the profession and position of digital forensics in society, education and professionally; educational principles and challenges; students and professionals as learners; and developing policies and frameworks. Where existing literature is used throughout to support research conducted within each chapter to continue to inform the reader of topical information and justifications or observations.

4.3.2.2 Action Research

Lewin (1946, cited in Coe *et al.*, 2017, p. 71) describes action research "as a way of generating knowledge about a social system while … attempting to change it". It is highly applicable in an educational context and often mentioned in academic works. It is described by Parsons *et al.* (2013, pp. 10–11) that action research is often categorised as applied research, however, can comprise of strategies from both basic and applied research. The authors describe the difference among these types of research, where differences include basic research being unbounded by a context and relating to the applicability of "principles, theories and frameworks" to other research, whereas applied research and action research take on a specific context, somewhat focusing on a level of problem-solving to explain a problem or phenomena (Parsons *et al.*, 2013, p. 11).

There are four steps at minimum authors define must be inclusive in an action research study (Sagor, 2005, p. 7) (Figure 4.3); although, there are further steps identified in the process by authors such as, Craig (2009); Tomal (2010) and Efron and Ravid (2013). This form of research is cyclical and often adept to re-assessing the outcomes to determine whether yearned changes have occurred, if not the process repeats.

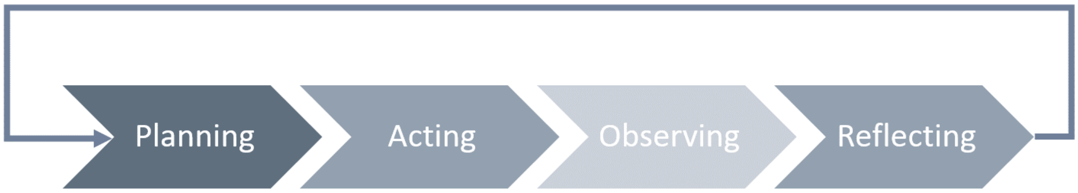


Figure 4.3 – The Action Research Process

This type of research is not bounded by either qualitative or quantitative research due to its position to present and implement change, where (Coe *et al.*, 2017, p. 71) describe claims that action research as a way to "bridge the theory-practice gap". In addition, Efron and Ravid (2013, p. 5) note how the "boundaries among theory, research, and practice are blurred" in the action research process, and much of the process is of a reflective nature.

Within this research, the purpose of action research is primarily the intention to improve practice through the insider (researcher) embedded within the context of the problem area defined. Thus, within action research participants are often involved and in control of the process. The researcher is inherently highly interactive and engaged in the process bringing unique positives and negatives to the process. The researcher (again, the insider) can bring to the table a knowledge richness, however, must be aware of the more extreme counter effects they can cause; for example, a higher level of subjectivity and the ability to be objective (Coe *et al.*, 2017). This leads to a demand for reflective practice and reflexivity by the researcher, including studying themselves in the process, where findings are directly applied to the insiders' practices. Another key consideration of action research in this study is the understanding of differing perceptions and interpretations of experiences within educational contexts. What the researcher experiences and what another subject, insider or reviewer might experience or interpret can be divergent (Coe *et al.*, 2017).

4.3.2.3 Grounded Theory

Grounded Theory (GT) is a way of thinking and conceptualising data collected in social settings and studies (Coe *et al.*, 2017, p. 100). GT was thought to be an important process within this study to understanding what is required in the digital forensic discipline to analyse the processes and outcomes of education. The process where "data collection, analysis and theory stand in reciprocal relationship with each other" (Strauss and Corbin (1990, cited in Coe *et al.*, 2017, p. 102); it is implemented when theming target audience experiences and integrating with literature surveys to evolve appropriate theories. GT also fits well with the data collection methods, outlined throughout these sections where, stages of analysis include coding (i.e. key points of the data), concepts (i.e. collection of codes of similar content), categories (i.e. broad ground of similar concepts) and theory (i.e. collection of categories that detail the research findings) (Ritchie and Lewis, 2003, p. 201). These are conducted across six phases discussed by Simmons (2010) and Glaser and Strauss (2009), seen in Figure 4.4. Stages involve breaking the data collected down into components which can be theorised into greater inclusive concepts. Making analytical and reflective memos, these resemble field notes, and help the researcher to build categories based on the identified concepts in order to form relationships and create theories (Glaser and Strauss, 2009). Constant comparative analysis/theorising is conducted across all stages (as depicted by overlapping boxes in Figure 4.4).

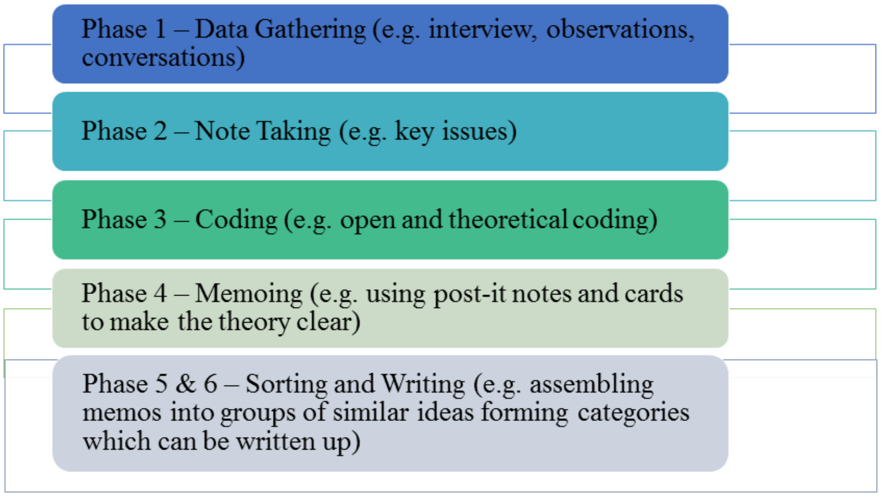

Phase 1 – Data Gathering (e.g. interview, observations, conversations)
Phase 2 – Note Taking (e.g. key issues)
Phase 3 – Coding (e.g. open and theoretical coding)
Phase 4 – Memoing (e.g. using post-it notes and cards to make the theory clear)
Phase 5 & 6 – Sorting and Writing (e.g. assembling memos into groups of similar ideas forming categories which can be written up)

Figure 4.4 – Grounded Theory Process

For the purpose of this study, open coding (i.e. analysis concerned with identifying and naming, categorising and describing content found through data analysis) is conducted throughout these phases. Open coding is the process of reading through the data collected, creating tentative labels (with ideal and appropriate naming conventions) for the chunks of data to summarise the findings (Seidel, 1998). Open coding seeks the direct meaning and is not subjective to existing theory (Coe *et al.*, 2017, p. 105).

Part of open coding relies on abstract and concrete categories to help generate a general theory or theories. In GT, coding is informal in its approach; an inventory of codes and descriptions is often useful to the researcher in coding multiple instances of qualitative data (e.g. transcripts, observations, conversations and so on). This approach to coding was applied due to this reason. Memos are written which discuss the codes and help with further theorisation and write-up. Memos and theoretical notes are going to be utilised much less in this research due to the amount of coding required across literature survey and data collection. However, these are reflected in the selection of categories and theories described in the writings of the findings. Recorded examples of participants' words are established with these codes for the researcher's mind and analysis to help identify and relate categories and theories to the research questions.

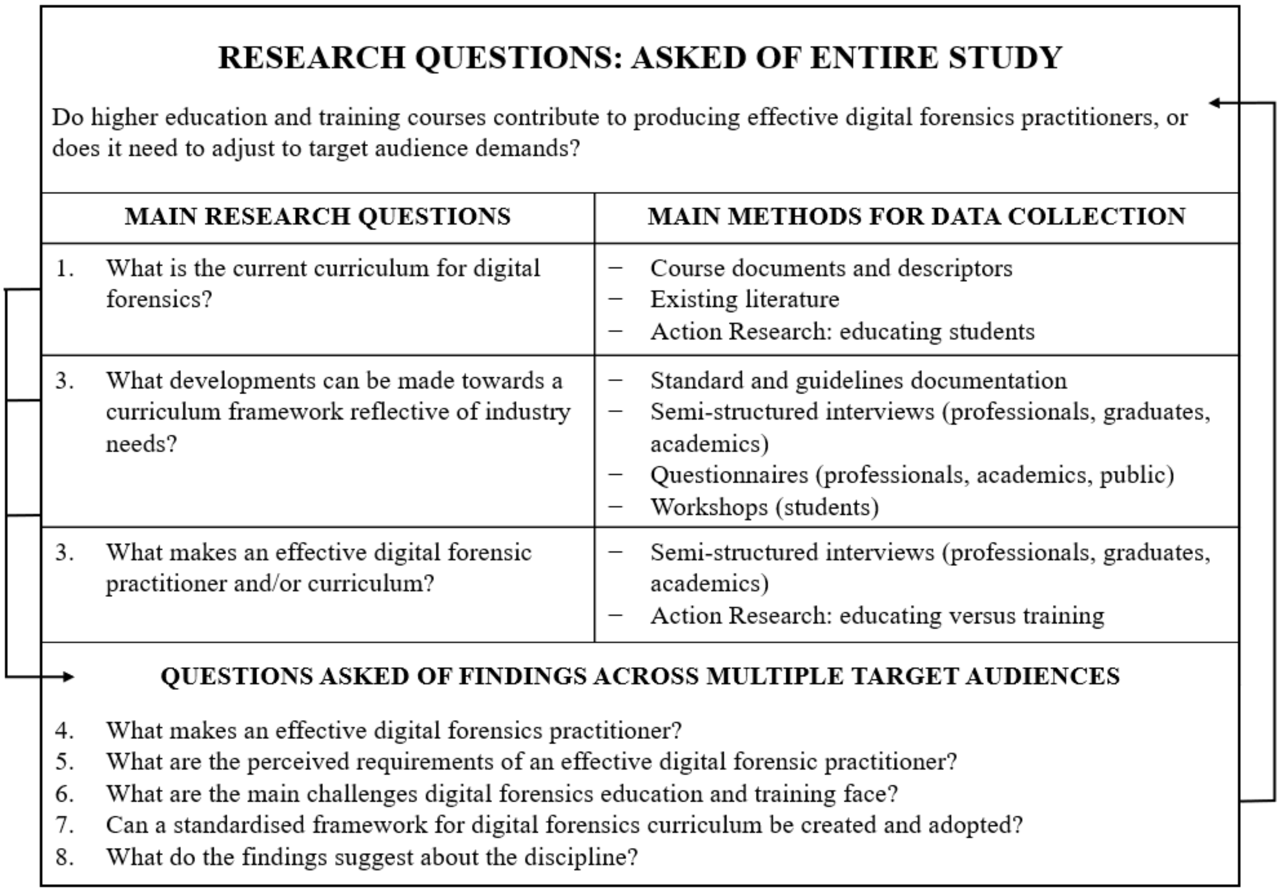
4.4 Research Design: The Methods Used

This section tackles the design of this research study. It seeks to consider the fundamental elements which are to be considered in any research, such as: purpose of the research; sampling; how the data will be collected and analysed; explanation of the obtainment of results; and the identification and acknowledgement of obstacles or problems within the research. Key considerations must also include acknowledgement of the audience(s) for the research, what and how much information is essential as well as sources through to availability and timescales.

Flick (2014) outlines a checklist to selecting a research design where focus addresses several components ranging from: the research questions in context of design and application, the research and methods in respect of researcher (i.e. do they have the skills to apply the design) and their participants (i.e. is the design appropriate for the target audiences), the scope and interaction, through to interpretation and discussion.

The focal point of this research is largely a qualitative research design, exploring phenomenon (e.g. situations, experiences and concepts) within digital forensics education and training. Further argument for a qualitative design is the need to understand the topic more in-depth, in context of its associated demands (i.e. keeping abreast with developing technologies and crime and employability from educational programmes). Analysis seeks to draw and generate answers to the abovementioned research questions where, little work socially has been undertaken to discover more in-depth aspects of officer training in practice and student education within the discipline. This research looks to explore this gap with more gravity.

Throughout, a range of methods are utilised including interviews, observations, surveys and literature reviews. Table 4.4 displays where these methods and different styles of research have been adopted to deliver this thesis.



RESEARCH QUESTIONS: ASKED OF ENTIRE STUDY

Do higher education and training courses contribute to producing effective digital forensics practitioners, or does it need to adjust to target audience demands?

MAIN RESEARCH QUESTIONS	MAIN METHODS FOR DATA COLLECTION
1. What is the current curriculum for digital forensics?	– Course documents and descriptors – Existing literature – Action Research: educating students
3. What developments can be made towards a curriculum framework reflective of industry needs?	– Standard and guidelines documentation – Semi-structured interviews (professionals, graduates, academics) – Questionnaires (professionals, academics, public) – Workshops (students)
3. What makes an effective digital forensic practitioner and/or curriculum?	– Semi-structured interviews (professionals, graduates, academics) – Action Research: educating versus training

QUESTIONS ASKED OF FINDINGS ACROSS MULTIPLE TARGET AUDIENCES

4. What makes an effective digital forensics practitioner?
5. What are the perceived requirements of an effective digital forensic practitioner?
6. What are the main challenges digital forensics education and training face?
7. Can a standardised framework for digital forensics curriculum be created and adopted?
8. What do the findings suggest about the discipline?

—adapted from (Coe *et al.*, 2017, p. 117)

Table 4.4 – Research Questions in the Context of Methods for Data Collection

This study is unable to observe every individual across each target group. Therefore, sampling is key to building a representation of what can be observed and further discovered and researched. Sampling is further discussed in section 4.4.6.1.

4.4.1 Interviews

> There are "no iron-clad rules of what constitutes sufficient data."
>
> —(Coe *et al.*, 2017, p. 187)

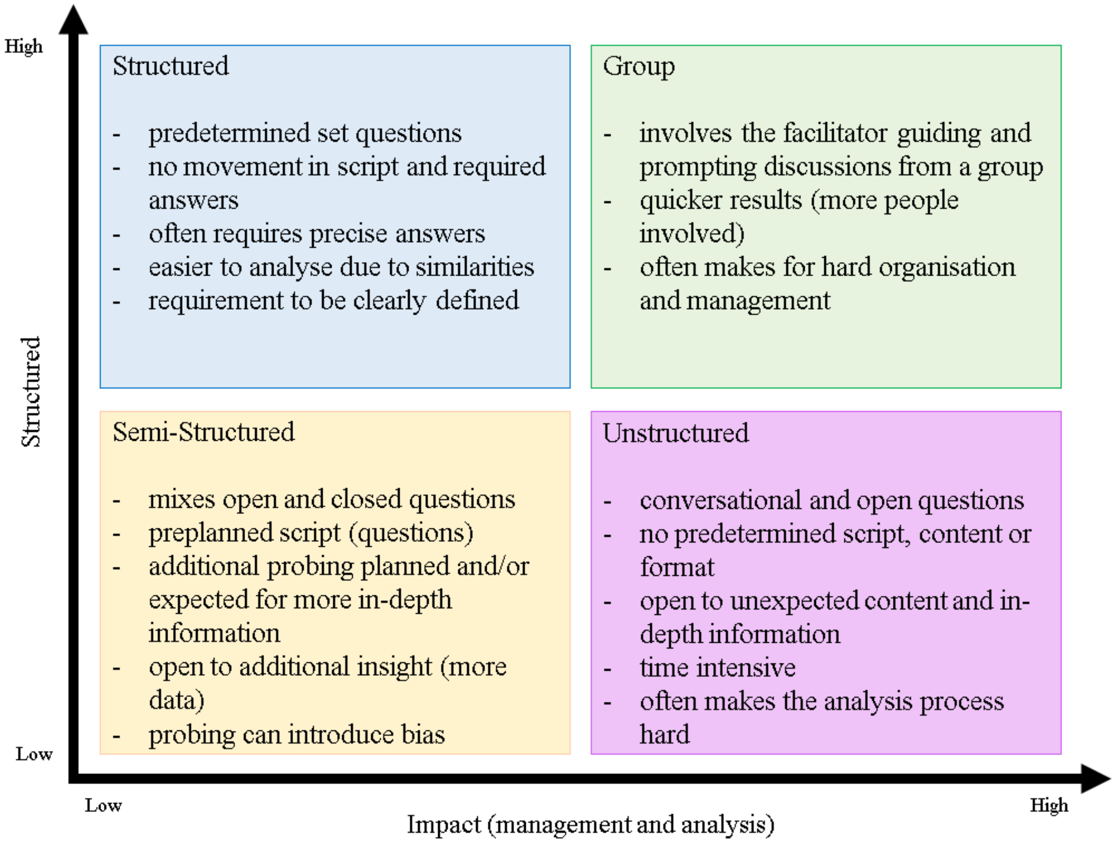
Interviews are the interchange of rich information between two or more individuals for a specific purpose which provide the researcher with the chance to purposefully interact with the participant and can often, by chance or planned, end in a more in-depth experience (Coe *et al.*, 2017, p. 183). Such a technique facilitates the use of multiple senses providing a rich variety of information for the researcher; this study focuses more on the verbal outcomes of these interviews. Interviews can take multiple approaches e.g. open-ended, guided/semi-structured, and closed/rigorously controlled (Minichiello (1990, cited in Punch, 2005, p. 169).

The researcher within this study is attempting to learn what the participant knows and has experienced of digital forensics in relation to effective practitioners, with a focus on graduates after academia. The researcher is also looking for what the interviewee feels might be of significance and key to understandings based on their lived and worked experiences. Control and structure of the interviews does not lend itself well to a restricted approach.

In a study like this where unique and personalised views, beliefs and experiences are sought after, more open-ended and semi-structured approaches take precedence. Such interviews provide greater flexibility and the notion to collect personal views and experiences. The use of open-ended and semi-structured interviews does not reduce, or eliminate, the planning required for interview sites, participants, questions, topics and objectives. To enable a successful interview some planning still exists, covering a multitude of factors. These are factors, which have an impact on the interview rapport, question format and language, researcher's position, the direct or in-direct nature of questions, prompts and probes, follow-up questions, motivations and so on.

This study adopts an interview strategy which is more directive and enables the interviewee to converse freely allowing for the initiation and potential for more in-depth or unexpected responses, experiences and topics. Thus, the interviews in this study align with a semi-structured approach with a tendency to lean toward unstructured territory (Figure 4.5).

The strategy of open-ended and semi-structured interviews allows for much greater flexibility to determine questions during the interview as a way of collecting quality rich information and further the use of probing mechanisms to gain more from the interviewee. The interviewer is free with semi-structured interviews to re-order, mix and omit questions, or even ask the questions in a different way depending on the context where more open-ended questions are used to facilitate supplementary questions (Adams, 2015). This can be successful in the data collection process; particularly where different social settings are involved. Similarly, the unstructured essence allows for a more informal approach and conversational stance allowing the interviewee to identify information freely and more in-depth with greater rapport having been built.



Structured

- predetermined set questions
- no movement in script and required answers
- often requires precise answers
- easier to analyse due to similarities
- requirement to be clearly defined

Group

- involves the facilitator guiding and prompting discussions from a group
- quicker results (more people involved)
- often makes for hard organisation and management

Semi-Structured

- mixes open and closed questions
- preplanned script (questions)
- additional probing planned and/or expected for more in-depth information
- open to additional insight (more data)
- probing can introduce bias

Unstructured

- conversational and open questions
- no predetermined script, content or format
- open to unexpected content and in-depth information
- time intensive
- often makes the analysis process hard

Figure 4.5 – Example advantages and disadvantages of popular interview methods

A limitation of interviews focuses on the time they require, and intensive nature be it face-to-face, or through communication software requires awareness of time taken to interview each participant, time to collect all data and review, and further then the time taken to analyse information gathered for reporting. This can therefore also be an inconvenience for participants, depending on the study requirements of each.

Furthermore, awareness of the rapport built between researcher and interviewee to build trust and gain rich information as well as the potential for interviewer bias is an element which must be considered and discussed previously. The openness of an interview and respondent views, experiences and discussions are reliant upon the rapport, the degree of directiveness (e.g., considering interviewer personality and position, interviewee responses and openness) (Whyte, 1984, p. 99), influences both internal and external influences and even social aspects and personalities. The position of the researcher is key and the impact they can place on interview questions and responses is an important consideration. As an interviewer control takes place prior to, during and after the interview. Questions determined prior to the interview can, to some degree, control the responses gathered during an interview if too confined. However, these questions can help to start the process and discussions with participants.

As a result of the researchers' own position and experience, respondents felt comfortable engaging in questions and discussion, technically and otherwise without querying the length and depths of the researchers' own experiences. In all the cases of interviews, contacts were made via convenience methods i.e., they were people the researcher or their colleagues knew. Contact was initially made via email, where the objective of the study was identified to the potential participant, along with a consent form and pre-information sheet. The consent form outlined the ethics of the study as specified by Canterbury Christ Church University, where participants are asked to consent to the interview process including recording if willing and the use of their accounts within analysis and write-up of the thesis. Furthermore, the pre-information sheet asked consenting participants to fill out a one-page document asking for their contact information,

Interviews within this study are conducted to help identify experiences and shortfalls of graduates toward their effectiveness of being a practitioner as well as experiences on-the-job to help identify what makes someone 'effective'. Themes are identified or created in the stage of data analysis among groups and audiences to inform discussion areas throughout this thesis. A majority of interviewees were happy to be recorded, except three individuals where notes were made instead. Interviews were then transcribed and analysed using manual process of analysis. The researcher opted for manual analysis via open coding with the feeling this would provide richer data where, it was possible software used to help could place between the data and the researcher's ability to synthesise themes and concepts.

4.4.2 Observations

To conduct measurements against the delivery and success of both training of police officers and education/training of students alike, observations as method are used in this study. Observations are deemed most useful for these circumstances to provide narratives to the delivery mechanisms, understanding the further outcomes of courses. Observing of the teaching/training and the learning styles of learners can obtain a deeper understanding of the situation and discipline as it stands. Within educational research, observations are most commonly used to study class behaviours, and commonly take on a quantitative approach. Similarly, to interviews, they are a timely cost for the researcher due to the likely necessity to observe participants on more than one occasion. Again, alike to interviews, the researcher can implement their own bias: 'observer bias', where own beliefs can influence the way one observes others. Not only can the researcher impose bias, they can also influence the participants: an 'observer effect', or otherwise known as the Hawthorn effect (Monahan and Fisher, 2010). This effect introduces implications on the behaviours of the participants, where they behave differently and are more conscientious than normal due to an observer being in the room (Monahan and Fisher, 2010). Tong (2004) notes this in his work, when training police detectives, cohorts of participants were against being recorded in training sessions; however, they did not mind notes being taken. If Tong (2004, p. 162) had recorded the detectives, they may have acted much differently on courses due to the feeling they felt towards being "on record and anything they said could be used against them".

Professionals in training settings as well as students in lessons and workshops were observed within this research by the researcher in the form of action research. The researcher discusses observations of these groups within this study, particularly the researchers own experiences in teaching digital forensics at higher education, often where problem-solving sessions were adopted. Notes were made when the researcher identified difficulties, views and experiences of target groups in their educational or training setting.

4.4.3 Questionnaires

Questionnaires are often used as a simple instrument for collecting opinions, most on a scaled approach as often seen within educational course evaluations. Although their simplistic delivery is the main foundation for their adoption, Leeuw *et al.* (2008, p. 1) writes that "[t]he idea of conducting a survey is deceptively simple". Questionnaires are a tool and are classified into two main types: open (i.e. unstructured) and closed (i.e. structured) approaches (Gillham, 2008, p. 4; Sesay, 2012, p. 78).

The use of questionnaires within this research are implemented at a very early stage across several target groups. The adoption of questionnaires further is pursued for the dissemination and collection of public perceptions on digital forensics and cyber security discussed in 4.4.6.1. Capturing the public's perceptions is key to rounding up the thoughts on the subject and its place within public awareness and education. With a wider audience it allows for diverging and extending themes for comparison across, and with multiple target groups.

It is commonly indicated that "a questionnaire should not be overly long" due to the cognitive limits and attention span of respondents (Adams and Cox, 2008, p. 19). Further to this, effects on the completion, and usefulness, of the data gathered is measured by the question, and type of question applied (e.g. leading or too many open-ended questions which can be overwhelming); again achieving what they believe to be a socially desirable behaviour (Kaminska and Foulsham, 2013). Due to the nature of the subject and goals addressed, limitations of questionnaires presented throughout this research relate to the length of the questionnaires disseminated and breadth of answers required (i.e. in-depth experiences and views) as depicted in Table 4.5. Respondents are known to often avoid a questionnaire or rush their responses if deemed too long (Adams and Cox, 2008). As a rule of thumb, therefore, questionnaires are expected to not exceed the 20-minute mark to reduce engagement depreciation of respondents (Cape, 2015, cited in Brace, 2008, p. 50).

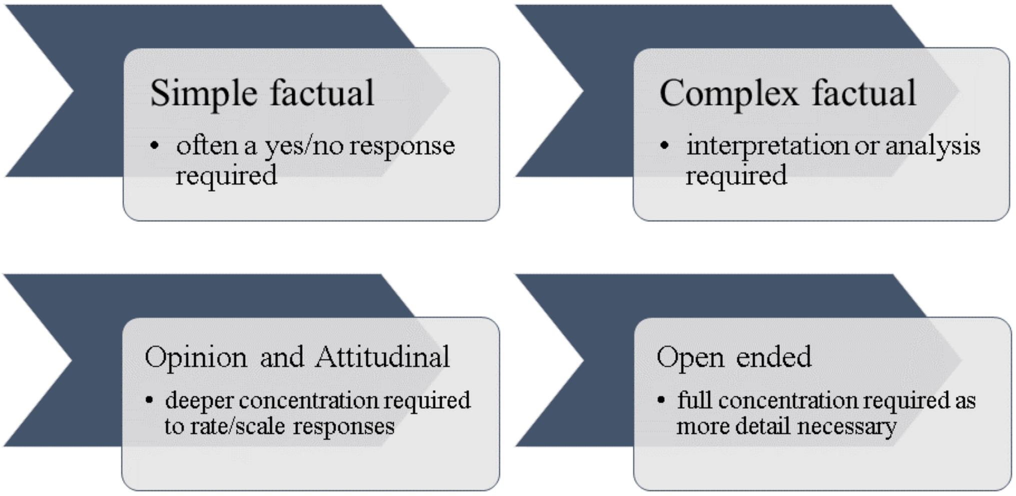
Limitations	Issues	Addressing Issues
Length of Questionnaire	→ Survey fatigue → Time taken → Data quality → Respondents are short with answers to open-ended questions → Respondents avoid questions or rush responses → Resources (time and effort) required → Response rate	→ Split into sections → Mix of question types → Limiting the number of questions asked to those of relevant topic and interest to the participants (to later reveal the results) → Skip over questions where possible yet still meet goals of questionnaire → Test response time
Type of Questions	→ Too many open-ended questions → Question focus	→ Mix of question types → Adequate space for participants to answer each question → Concise wording → Skip over questions if possible

Table 4.5 – Limitations of Questionnaires Utilised in this Research

To address concerns with the usability and effectiveness of long questionnaires, designs leaned toward structured and manageable blocks (i.e. sections sought to help ease completion and create groupings for the respondents) as a progressive reveal as not to swamp the participant. Furthermore, this is noted by (Adams and Cox, 2008, p. 19) to not only "help the respondent contextualize the subsequent questions … [but also help the researcher] identify how the sequence [] affect[s] the respondent" and ease data analysis. Within this research the four question types mentioned by Adams and Cox (2008, p. 20) are utilised and include those depicted in Figure 4.6 (below).

Many open responses are sought across questionnaires in this research to achieve a range of goals, largely in accumulating experiences and views. This can make for a challenging response rate often due to resource intensiveness on behalf of the respondent (e.g. their time, interpretation and analysis and descriptions). These types of questions require much more, and thorough, consideration by the participant and researcher alike.

From the researcher's perspective the downside of these type of questions are the difficulties in analysing answers to compare, critique or even categorise. Considerations for the management of interpretation of answers is also an element of concern. Although, the positive rewards of these questions are their ability to facilitate and allow respondents to answer in detail and clarify their response(s), build trust with the respondent, and allow them to feel unrestrained. Further still, they allow for unexpected content which can similarly be seen in unstructured interviews.


Simple factual

- often a yes/no response required

Complex factual

- interpretation or analysis required

Opinion and Attitudinal

- deeper concentration required to rate/scale responses

Open ended

- full concentration required as more detail necessary

Figure 4.6 – Four Main Types of Question in Questionnaires

4.4.4 Workshops

Typically, a workshop in the educational or training setting consists of an arrangement where a group of people interact performing problem-solving or innovative tasks in relation to a specific issue (Oxford University Press, 2014). In this research, workshops are used in an academic setting with new students within the discipline. The workshops consisted of a questionnaire to gain the students views on the subjects and their career progression ideas, as well as a short presentation to provide students with some findings from other target audiences. Subsequently, the points of the workshop were discussed by the group and academics present.

The value of understanding, and the value, of the students' perspectives of the domains should not be dismissed; within this research they are deemed to be important in understanding the expectations of programmes within the sector from a student perspective. Limitations of this workshop questionnaire approach have been listed above. At the end of each workshop the researcher and the students came together to discuss responses provided to the questionnaire. A progressive reveal style implemented to reveal the students' responses and discuss their views in more depth. Short workshops also allow the researcher to discuss aspects which may be of use to students as they progress through their study, including aspects of employability through the discussions of the students' responses and those of participants in the four other target pools.

4.4.5 Statistical Analysis

Although this research adopts a qualitative approach, chapter 8 adopts several quantitative approaches; typically, statistical methods. In this example, student workshops are expected to lead to statistical analysis of the topics which students feel are important on a course targeting digital forensics. This statistical analysis is expected to help identify key aspects and topics which can be made as comparison against the more qualitative approaches addressed throughout the rest of this research. Adopting an approach where quantitative research is embedded within a qualitative approach.

Statistical analysis in chapter 8 is presented in the form of techniques such as Frequency/Descriptive Analysis and Principal Component Analysis (PCA). This study uses these techniques due to the main practises including understanding variable structures and data reduction to "a more manageable size while retaining as much of the original information as possible" (Field, 2013, p. 666).

4.4.5.1 Descriptive/Frequency Statistics

Descriptive statistics are the most commonly used statistics and are used to summarise the frequency or measures of central tendency (Walker and Maddan, 2009, p. 91) . The frequency shows the number of occurrences and calculates central tendency such as, the mean. In chapter 8, these statistics are used to answer the research questions *what is the student curriculum for digital forensics?* and *what developments can be made towards a curriculum framework?* Each of these questions looks at topics and skills sought from a programme, student and graduate studying in digital forensics and cyber security. By completing frequency analysis of all the data captured from the target group: students, descriptive statistics will allow for findings of topics students perceive as important in such a degree at early stages of their studies. Cumulative frequency will be particularly useful in identifying higher rated topics by importance ratings by respondents.

4.4.5.2 Factor Analysis/Principal Component Analysis

It should be noted, for FA and dimension reduction techniques like PCA to be considered an appropriate analysis technique, participant numbers greater than 50 are expected (de Winter, Dodou and Wieringa, 2009). As a general rule of thumb both Kaiser-Meyer-Olkin's (KMO) , a measure of sample adequacy, and Bartlett's Test of Sphericity, a hypothesis test, are calculated to check how suited the student data is for conducting factor analysis.

KMO is a statistical test which returns values between 0 and 1, where the test measures and indicates the proportion of variance among variables, i.e. do the variables share a communality (Field, 2013, p. 684). Bartlett's Test of Sphericity on the other hand is also used to examine relationships and validity/suitability of the data (e.g. student responses). It is utilised to test that the correlation matrix is not diagonal, and a significant correlation exists, checking for redundancy between the variable which can be summarised by a few factors (Field, 2013, p. 685). Testing two hypotheses regarding interrelationship.

- Null Hypothesis H_0: There is no significant relationship between variables affecting the choice of subjects.
- Alternate Hypothesis H_1: There may be a significant relationship between variables affecting the choice of subjects.

For these methods of analysis to be validated KMO must be greater than 0.6 and the significance (p) in Bartlett's Test less than 0.05 (IBM Knowledge Center, 2014b). Where the significance is less, it indicates there are some relationships between the variables to include in analysis. In this case the significance is less than $p<0.05$ and indicative of the test's potential suitability for factor analysis (Field, 2005). The null hypothesis H_0 is rejected at this stage, accepting the alternate hypothesis H_1 that there may be a statistically significant relationship between variables.

PCA is a dimension-reduction technique which relies on the orthogonal transformations and "aims[s] to reduce a set of variables into a smaller set of dimensions (called … 'components')" that still contain most of the information of the initial, much larger data set (Field, 2013, p. 667). PCA is a mathematical calculation which seeks linear combination of the variables in the dataset as weightings (Kaplan, 2004, p. 10; Field, 2013, p. 671); where, the maximum variance amount, common and unique variances are analysed and can be extracted. It converts possible complex correlated variables into a set of values linearly uncorrelated called principal components (Linting and van der Kooij, 2011, p. 12). There are several merits and de-merits of this type of analysis; merits include reduction in size of data, estimation of probabilities with no need to assume independence, and rendering of uncorrelated component sets to find hidden linear correlations (Karamizadeh *et al.*, 2013). This removes what Karamizadeh *et al.* (2013, p. 174) state as 'noise' and filters out the important regularities within the data, while often being used to standardise the data.

The technique is most useful when interpretation of relationships between objects is hindered by many variables. Reducing the dimensionality leads to interpretation of fewer components than the initial number of variables. De-merits can include its restriction to linear models, assumption of scale where, its complexity can also become a hindrance in interpreting the data (Linting *et al.*, 2007, p. 12).

In this study, PCA is to be utilised with ordinal type data in the form of Likert scales, where more than 20 topics are measured using the same construct. In order to validate these, PCA is used. Field (2013, p. 676) signposts to the literature that although other methods such as Factor Analysis can be used instead of PCA, it is suggested that

> "the solutions generated from PCA differ little from those derived from factor-analytic techniques … with 30 or more variables and communalities greater than 0.7 for all variables … however, with fewer than 20 variables and any low communalities (<0.4) differences can occur".

When calculating PCA, rotation is used to adjust the factor axes to achieve a simpler, more meaningful solution. The rotated component matrix contains estimated correlations between each variable and the estimated components found when calculating PCA. The *loadings* are the correlation coefficients between the variables (rows) and components (columns) which are used to calculate the *eigenvalue*; the eigenvalue being the sum of squared *loadings* for a component (i.e. the amount of variance by all variables accounted for within each component) (Jolliffe, 2002; Field, 2013). Jolliffe (2002, p. 131) states the cut-off for points to consider as 0.7. A *scree plot* is then used to plot eigenvalues (Y-axis) against component values (X-axis); it is suggested that the cut-off point for components to consider is that where the graph slopes dramatically (the 'point of inflexion') (Field, 2013, p. 698). Rotation of components axes are utilised as un-rotated components axes may not align well with the pattern of variables. This results in a lack of clarity in variable patterns. A rotated axes solution provides a more meaningful correspondence of variable patterns yet preserving their relative relationships. Thus, rotation keeps together the items that are closely related and separates them clearly from other items/groups (Field, 2013, p. 790).

There are other procedures such as Categorical Principal Components Analysis (CATPCA) which can also be used to quantify categorical variables while reducing data dimensions (IBM Knowledge Center, 2014a). This method can be used on "complicated multivariate data, consisting of nominal, ordinal, and numerical variables" (Kaplan, 2004, p. 50). One advantage of CATPCA are its graphical representations, where several authors note the program "renders more insightful (bi)plots than standard linear PCA" (Linting and van der Kooij, 2011, p. 24). However, for this study PCA is used as a first step in analysis to reduce the number of topics, known as subjects in CATPCA, and identify those which students perceive or feel are important on a degree in digital forensics and cyber security.

4.4.5.3 Why these Methods, and Other Methods Explored

This section outlines why the methods discussed above were selected as the most preferable research design in comparison to other methods/options which were considered. Different research designs such as using focus groups or ethnographic studies were contemplated and are discussed below.

Due to their capacity to fit into existing practice workflow, and the combination of stakeholder groups in synergy with one another, focus groups were thought-through. Focus groups are defined as an interview which are used to obtain perceptions on an area of interest in a small group environment (Creswell, 2014, p. 243). While discussions are prevalent, Patton (2002 cited in Creswell, 2014, p. 243) states the method "is not a problem-solving session [and] It is not a decision-making group." However, focus groups allow for group discussions in the normal ways in which people express and produce ideas/opinions and allow for validation of these among several individual experiences.

Focus groups are often used in similar examples of qualitative research as an alternative to in-depth interviews, particularly when exploring the culture or social context of an issue across a range of subject areas (Ritchie *et al.*, 2013). Positives of the method allow for snowballing between the groups of individuals and may be a quicker approach than individual in-depth interviews. They are used to elicit information from a group that enable researchers to explore combined and, sometimes local, perspectives, however, they are not a reliable technique to determine what an individual has experienced or their views in more depth. Further limitations include:

- organisational effort, access, and accommodating/meetings to suit all participants
- they allow for a limited number of questions
- note-taking issues
- problems mediating the group discussions
- dynamics and integration of members in a group (one individual can dominate the discussion or sway the tone and views of the entire group)
- loss of individual responses and later access, interpretation, and analysis
- potential to capture fewer individual in-depth responses and in turn experiences.

While focus groups are useful for collecting and assessing conversations and combined opinions, the limitations of focus groups were considered by the researcher and concluded that focus groups would lead to further interviews or questionnaires on an individual basis. Furthermore, deliberating the highly sensitive industry and possible issues with a range of access in person and timely as a group, focus groups were eliminated as a potential design.

Ethnographic studies that consider both groups and individuals in natural settings over a longer period of time were also considered. Ethnographic studies allow the researcher to become part of the environment and observe social phenomenon and even join in with activities while taking a range of notes and recording observations and themes (Creswell, 2014, p. 319). Limitations include:

- representative sampling and gaining access
- length of time required to conduct a study
- engagement between participants and the researcher
- demands of fieldwork and observations on the subjects and organisations
- potential bias added from the presence of the researcher within the environment
- privacy issues during observations.

Again, issues such as gaining access, a highly security orientated industry and limitations with potential observations were considered too problematic in light of the need to gain experiences, views and opinions from a range of stakeholder groups and individuals.

For these reasons, interviews and questionnaires were deemed the most appropriate techniques particularly when considering the range of access issues which could arise when sampling for participants.

In addition, original design activities for students included activities such as, card sorting to design a course as well as mind mapping thoughts and experiences, however, with the potential number of students and short timescales available and restrictions to labs or lecture times meant an online questionnaire seemed more fitting for each university participating. Further to this, a questionnaire would allow for comparison and immediate post-mortem analysis of student responses and promote on the spot discussions while also comparing and critiquing with responses previously gathered from varying target groups.

4.4.6 Participants, Sample Sizes, Gaining Access and Site Selection

This section describes the researchers' approach to gaining access to participants and highlights key characteristics of the participants themselves.

4.4.6.1 Sampling

The rich information drive for this study stimulates the necessity for non-probability sampling for the interviewing of participants within the selected target groups sought to be of use due to their knowledge and link to specific purposes to the research in this study. Probability sampling methods were unsuitable for this study, in that such approaches are based on the selection (usually random) from a larger population based on probability (statistical theory). The target groups identified within this study are not conducive to this method as a larger population is sporadic and unknown due to the disciplines broad and non-adhesive alliances. However, there are three main techniques used under the umbrella term of non-probability sampling; in this study, both convenience and purposive methods are utilised.

After identifying the target groups, sampling of interviewee participants could take place. In order to capture views from a wide range of participants, convenience sampling through personal contacts was adopted, where the selection of respondents by opportunity for the nearest useful captive audiences were seen. An everyday example would be the use of close friends, who the researcher has ready access to; these participants are likely to agree to participation due to the relationship shared between researcher and individual outside of the study process. When considering the stakeholders in this study, convenience sampling is of specific focus for alumni from the digital forensic degree programme at Canterbury Christ Church University. Due to data protection (Council of Europe, 2016; *Data Protection Act*, 2018), access to personal details of previous students on the programme would be infeasible, therefore alumni contacts known to the researcher and colleagues that will satisfy this target group. Attempts were made through alumni relations to access participants for this study, however, little response (one participant) was seen.

Furthermore, it was key to adopt purposive sampling techniques to select participants whose knowledge basis is specific to the purpose of the study. Purposive sampling involves the researcher's personal judgement to choose relevant respondents. Therefore, this study focuses on choosing people within each target group who would be best to assist the research. For example, rather than sampling a wider population and including a vast demographic of individuals, specific focus is placed on those within digital forensics in industry and those involved in its associated streams of education and training. This method can influence a level of researcher bias, due to the necessary existence of advanced knowledge of the target audience(s). However, rather than placing focus on the aims and theories the researcher strives to achieve, emphasis is greater focused on the criteria used to select and accept respondents to reduce the researcher's bias.

Participants were selected and sought using open calls via email communications which targeted a range of individuals listed on for example, company pages, university websites, etc. Furthermore, social media and digital forensic forums were used as an open call for participants through convenience sampling which led to calls for participants communicated between the researchers known contacts as well as contacts of colleagues. In addition, graduates were sought after through alumni relations at Canterbury Christ Church University as well as connections mentioned above.

With convenience sampling in this example there is possibility for all those involved to be related to the researcher's home institution, and the potential to introduce implicit bias in the experiences drawn upon which inform opinions. This study captures experiences from a range of stakeholders, and while individuals may have connections to the researcher's organisation or colleagues' opinions and experiences will be drawn upon from their own workplace, be it industry or another academic institutions as well as their experiences with a range of education and training. The stakeholder groups with the highest possibility of implicit bias are graduates and students, due to their experience with education from the researcher's organisation.

Characteristics of qualitative research often lead to a small number of respondents as identified within this study. This study does not require a mass quantity of interviewees; what is often of more importance is the significance of achieving a strong coverage of the society within each target population acknowledged. Although each target audience has been acknowledged within this study, a strong sample size which would be required in statistical analysis is not feasible due to the high security and demanding roles which digital forensics employees are bound by. Thus, where data saturation exists, e.g., a point where similar recurring themes appear the number of interviews and questionnaire responses are halted and perceived enough. Characteristics, behaviours, experiences, opinions, and beliefs can be identifiably different within, and contrasting, each target audience within the discipline and must be considered in this scenario as a limitation.

The idea of data saturation is emphasised within this study, this is where the researcher stops collecting data when categories/themes become overloaded and repetitious e.g., discontinuing data collection and/or analysis when the categories and themes recur commonly among data collected (within and across target groups) and lack new properties of insight (Saunders *et al.*, 2018).

4.4.6.2 Participant Information

Stakeholder	n
Academics	16
Students	43
Graduates	7
Professionals	33
Public	102
Total	**201**

Table 4.6 – Number of Research Participants

While demographic details of participants are included within chapters of this research or referred to in Appendix B, this section draws on the overview of participants across this study. Table 4.6 (above) separates the number of participants in this study by each stakeholder considered within future chapters of this thesis.

A large proportion of the participants in this study were questioned online, however, interviews which ranged between 20 minutes and 2 hours were conducted with eighteen participants face-to-face and one via email. Each interview took place at a site convenient for the interviewee which included campus locations through to local coffee shops on a non-formal basis.

Each chapter demonstrates participant details including information on analysis methods applied such as, role, gender, years' experience, and site of interview, or discusses the use and proportion of people involved in questionnaires. Further participant details can be found in Appendix B.

Online participants in this study included 102 members of the public, 7 academics and 30 professionals. Further, workshops were conducted at anonymised universities which took approximately one hour. Students were asked to complete a questionnaire and partake in a post-mortem of their results where discussions could be applied (discussed in section 4.4.4). Furthermore, general teaching and learning observations were made by the research during several educational and training settings where action research is applied, the number of students within these settings differed. Typically, observations were made of level 5 and 6 students within digital forensics higher education and law enforcement officials in training environments.

It should be noted that expected numbers for this study are low where it is expected that most responses would veer toward identification of the male gender particularly for four out of the five target groups. Participant information demonstrated in each relevant chapter and, data concerning workshop and online participants (Appendix B) support this expectation. Female participants were not excluded by the researcher while gaining access to contributors. Gender imbalance in technical roles such as, particularly digital forensics and cyber security are often noted; where, in a 2017 study, it was reported that "the total number of women employed globally in the cybersecurity profession stands at 11%" (Frost & Sullivan, 2017, p. 6). The study also reports that women who entered into the cyber security domain held higher educational qualifications than the men with undergraduate degrees ranging in computer and information sciences through to mathematics, engineering and social sciences (Frost & Sullivan, 2017, p. 10). The lack of women positioned within these roles is suspect to several effects, including the male-oriented history of computing and policing, and potentially the mental and emotional impact of illicit and disturbing materials which may be handled daily, particularly in digital forensic roles. When looking at the history of digital forensics and the literature, it is apparent that the role of a digital forensic practitioner has developed from a police-orientated background. Throughout the history of policing, the number of roles which women have occupied have been low but nonetheless these have gradually increased. Today it is reported that, in England and Wales alone, "61% of police staff" are women (Hargreaves, Husband and Linehan, 2018, p. 35). What these statistics do not identify are those in more technical positions such as, digital forensics or cyber roles. From the authors perspective, the identity of women in digital forensics has started to grow, although assumptions can be made that there are still more men than women within the continuously developing discipline.

4.4.6.3 Gaining Access

When dealing with target groups, gaining access is a key component to achieving a 'good' sample size and 'good' meaningful results. Although, sample sizes can only truly be calculated when the population size of each target group is known. In this research the population size of each group is vast and largely inaccessible, gaining access is therefore particularly hard in these circumstances even when based on convenience.

Gaining access professionally in a policing-orientated environment is a boundary when interviewing police officers both in and out of training environments. As Tong (2004, p. 167) notes the "hierarchy of the police organisation involves a complex web of gatekeepers which can create problems for researchers". This study found this to be a building block hard to overcome. Gaining access to professionals was slim for interview purposes although a convenience sampling method was employed.

To increase the number of professional responses several emails were distributed to well-known companies and police forces across the UK dealing with digital forensics seeking response to a professional questionnaire. In addition to this, posts on social media and digital forensic based forums were posted to entice more responses (see Appendix H - J.2). Several participants were gained from private and public sector departments via these methods.

In other cases, particularly responses from automated contact points of UK police forces boundaries and hurdles were still paramount. Where there were no specific contact points for DFUs within the policing branches, public access contact forms or email addresses were used for several UK-based police forces. Many responded with a response which stated the request had been sent on to the relevant department, however, the real success of these is unknown due to the anonymity of survey participants. Other outcomes led to no success.

One response stated:

> “Thank you for your email []. [We] do not open links to untested electronic surveys, therefore, we are unable to forward your email.”

After enquiring further if there was anything which the researcher could do further or contact which could be made with the department, the response followed:

> “Unfortunately, as I am sure you are aware, there are currently limited resource within many police forces across England and Wales. Completing a survey is not a policing purpose; the function of this office is to disclose police information held, where legislation allows or obliges and not necessarily to forward a link to officers who may wish to complete a survey. You may wish to request police information held under the provisions of the Freedom of Information Act 2000. I trust this clarifies and assists.”

The many pressures of police forces in the UK and lack of importance of a questionnaire is understandable in these situations, however, the need for research and the lack of information which the researcher saw to be gained from a Freedom of Information Request led to the understanding further that responses were likely to be short and low in numbers.

Where interviews, observations and workshops were conducted, the selection of sites were controlled through the convenience of the participants and target group type e.g., students, workshops would be conducted within their academic environment. In some cases, such as training of police officers and the education of undergraduate students, the site fell to the establishment where courses were conducted e.g. Canterbury Christ Church University. Furthermore, when interviewing people within industry and law enforcement, it was key that the researcher interview at a site beneficial for the respondents or even through electronic means.

4.4.7 Thematic Analysis

Throughout this research manual open coding has been used, where thematic analysis is utilised to see patterns and themes in data obtained throughout methods used in this research; such as, interviews, literature surveys, observations and questionnaires. These patterns and themes are important to answer the research questions. Open coding is the initial stage of qualitative data analysis where the data gathered is read through to create labels which summarise what is happening based on the meaning of the data as it emerges e.g., participants words. In this research open coding is used with inductive process inquiry in the effort to, as described by Thomas (2006);

- condense extensive and varied raw text data into a brief, summary format;

- establish clear links between the research objectives and the summary findings derived from the raw data; and
- develop of model or theory about the underlying structure of experiences or processes which are evident in the raw data.

Coding throughout this research is systematically conducted manually using highlighters, pens, post-its and through taking notes and memoing (examples depicted in Figure 4.7 and 4.8).

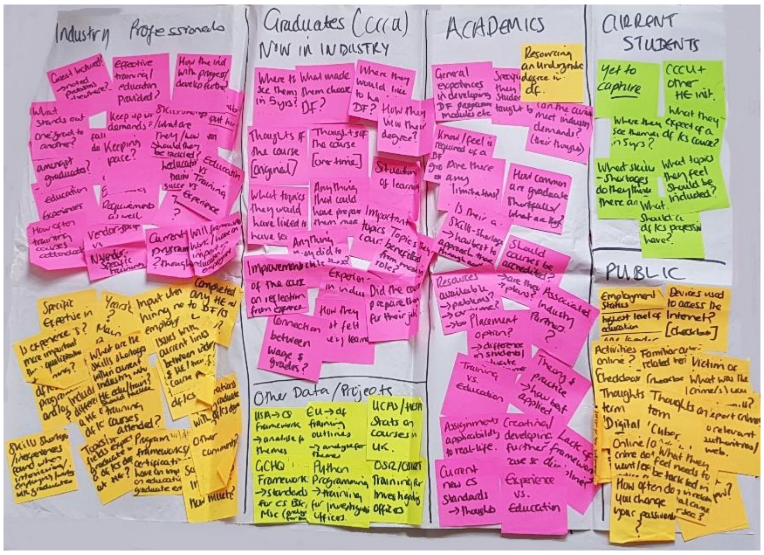


Figure 4.7 – Sticky-notes used to help identify the relationship of questions across target groups

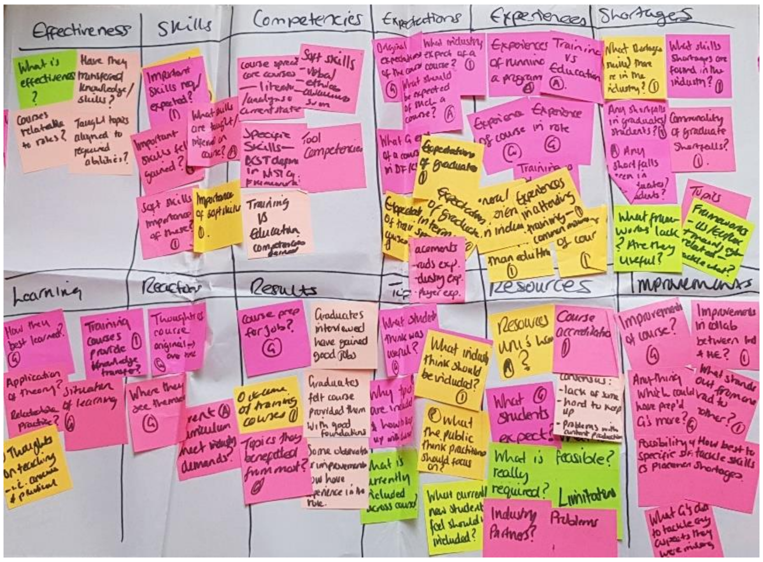


Figure 4.8 – Sticky-notes used to help identify the relationship of results based on target group and key themes/dimensions

Organisation and description of the data is crucial in fulfilling these steps of thematic analysis. Analysis goes far beyond identifying phrases and looks at recognising the importance and interpretation of ideas, concepts, and specific areas of interest in relation to one another across each target group.

Authors such as, Boyatzis (1998) identify that thematic analysis has "four distinct stages in its development" and discuss different approaches to thematic analysis. However, authors Maguire and Delahunt (2017) discuss "the most influential approach" to be six major phases described by (Clarke and Braun, 2013; Clarke and Braun (2006) cited in Maguire and Delahunt, 2017). These stages concentrate on identifying themes or patterns among the data captured. Phases include:

1. Familiarisation with the data: transcribing data where necessary, reading/re-reading the data, noting down initial ideas,
2. Generating initial codes: coding interesting features across the data, collating data into relevant codes,
3. Searching for themes: collating codes into themes, gathering data relevant to each theme
4. Reviewing themes: checking the themes work with coded extracts and the entire data set (i.e. how do the themes support the data and research); where necessary this step will be repeated if analysis is incomplete; generating a thematic map of analysis
5. Defining and naming themes: on-going analysis to refine and define each theme and analysis; generate clear definitions and named themes to identify which aspects of data are captured and their interests in relation to the research being conducted
6. Producing a report: selection of extracts and themes relating to research questions and literature (i.e., what data makes a meaningful contribution to answering the question or phenomenon, and why those themes are most useful); questioning themes and findings to check they are an accurate representation; writing up the analysis.

4.5 Summary

This chapter has focused on the methodologies and methods applied throughout this research, concerning the reader with several justifications and limitations among data collection and analysis, delivery of narrative through to sampling mechanisms. Multiple methodologies have been considered stressing the use of literature survey, action research and grounded theory. Methods have also been chosen and outlined including, interviews, observations, workshops and questionnaires which work in tandem throughout data collection and in producing the findings delivered in later chapters. An overview of analysis methods using thematic analysis has been provided, emphasising the use of manual open coding as an approach to help devise theories pertaining to the research questions originally outlined to support results embodied in the subsequent chapters.

5. Digital Forensics: Academic Challenges

Introduction

While a vast number of universities have taken the opportunity to offer courses in digital forensics and cyber security there are several challenges experienced by many. Some issues have been discussed in chapters 2 and 3, predominantly focussing on the lack of widely adopted curriculum frameworks within the discipline of digital forensics, alongside the challenges the discipline faced in establishing itself as a distinct academic discipline. Furthermore, literature highlighted that learning within the discipline is often practical in nature and incorporates a multitude of learning styles, it could learn from similar practice based and long-established disciplines such as medicine. While these challenges are recognised, continuing to fulfil the needs of any degree programme can be complex where procedures, standards, budgets, and resourcing are limiting and where a discipline is costly when balanced with more traditional studies. This chapter focuses on the continuous challenges that a technical course encounters while endeavouring to produce skilled individuals for industry. Looking at results from 7 questionnaire responses and taking onboard views gathered from academics (n=9) within the discipline through semi-structured interviews.

5.1 An Exploratory Study on Resourcing a Digital Forensic Course: Results and Discussion

Dedicating computing space to one programme can become a tough task, particularly where enrolment numbers are restricted by resources and space is required for multiple uses, and often multiple programmes. In computing, a workspace filled with computers is a requirement of the trade; however, at a higher institutional level these spaces may often be seen as generic student labs. There may also be argument here that computers are not necessarily a tool for the trade, and this is changing, where the use of laptops for digital forensics and cyber security are becoming the norm particularly when on the move. It may also be argued that laptops for student learning may suffice where free and open source tools are utilised. Results below highlight responses from several academics approaching the use of such spaces, issues presented and methods which have been taken to tackle these issues.

5.1.1 Recap on the Method

In late 2014, a preliminary study in the form of an online questionnaire was conducted to identify the resources, expenses, and student numbers of digital forensic courses within the UK. The questionnaire was distributed to a number of UK universities listed on UCAS as offering a course under the umbrella term 'digital forensics'. Discussions were made with attendees, mainly digital forensic academics, at the '10th Annual Teaching Computer Forensics Workshop' (Stephens and Humphries, 2014) to obtain their views. The aims were to find out current student numbers, resources (both hardware and software, people, and time), accreditations, resource updates, issues, and experiences of running such a programme.

The statistical and formative questionnaire was split into three sections to assess programme specific information from academic participants. The first section asked for general programme information, the second was divided to ask for information relating to laboratories, hardware and software, accreditation, and staff resources. Finally, the third section asked for general comments.

Seven academics, ranging from senior lecturers to heads of schools responded from seven institutions. There were many similarities, such as the quantity or specifics of course resources available and responses highlighted requirements of such a technology reliant course. This study highlighted how further research in this area should include additional mechanisms, for example interviews; something the author of this thesis embarks upon in following chapters. Participants of the online questionnaire provided current student figures per annum on digital forensic programmes to be between 10 and 50 students. In comparison to many other disciplines, these numbers may seem low for a HE course, however, as demonstrated in chapter 2 they are standard for digital forensic courses across the UK. One respondent noted student numbers between 80-100 per annum, a number which most institutions could not manage for several reasons discussed throughout this chapter.

This chapter also draws on semi-structured interviews conducted with academics who have experience of designing and delivering courses in the digital forensic arena. The uptake for interviews were small and thus may not be described as representative of the digital forensic academic community. Although, it should be noted that data saturation during thematic analysis discussed in section 4.4.7 meant that a large quantity of interviews were unnecessary. What these interviews enable are prompt discussion and narration of experiences for analysis and critique, and by means of collation with other target group experiences described throughout consequent chapters.

5.1.2 Dedicated Space and a Sense of Belonging

Dissimilar to subjects which strive on a continuous use of the traditional lecture based teaching method, computing subjects require practical and scenario/case driven learning in combination with theory (Irons, Stephens and Ferguson, 2009). This style often suits lower class numbers and is restricted by the maximum capacity of a laboratory environment and the limitation of academic staff available. These properties reduce the number of students who may be enrolled on a course at any one time or increase staff contact time by holding multiple tutorials when lab spaces are insufficient. Participants were asked how many computer labs existed in their respective departments, results show between one and twenty labs with each containing between 24 and 48 computers (Table 5.1 below).

Laboratories		**Computers**	
Number of Computing labs in departments	Number of labs containing specialist forensic equipment	Number of, in general Computing labs	Number of, in Forensic Computing labs
7	1	24	24
15	1	48	32
12	2	25	28
8	3	25	25
1	1	35	-
20	4	30	64
10	3	25	25

Table 5.1 – Laboratories and Computers in Respondents Departments

Often expectations are profoundly focused on those of HE rather than the subject itself, where authors Kinnunen *et al.* (2018) describe a "growing appreciation" of student perspectives in STEM based subjects. Referring to the literature (Douglas, Douglas and Barnes, 2006, p. 252; Tomlinson, 2017, p. 452) several contributing factors are identified when students contemplate and determine the value of their higher education experience. These range from the level of service, lectures and materials, teaching quality, sense of belonging and staff interaction, through to facilities (including "furnishing, decoration … and layout") and the high ranking of, in general, IT facilities (Douglas, Douglas and Barnes, 2006, pp. 252–257). For example, satisfaction that the course justifies the expense of more than £9,000 per annum. In a discipline where resourcing is often one of the subjects most prolific issues this can be challenging. Such expectations are duly minimised by technology on show, the specifics and number of laboratories and their access through to the expense of new buildings and vast technologies and dedicated spaces.

The author's own experience confirms this where, in recent years, students have calculated the cost of their contact time at university and assessed the available laboratory space and building aesthetics for perceived value for money[14]. While calculating these costs may provide students with an insight into the money they are spending it is not straightforward, particularly where technically driven subjects such as computer forensics are shaped by vast monetary expenses such as, high software and hardware costs beyond a traditional lecture based course offering, which may be suited for higher student numbers.

Angelopoulou and Vidalis (2015) have "argue[d] that for students to learn effectively and in depth, they need to feel as being valued and belonging." A sense of belonging may often be approached by dedicated spaces, where students feel a sense of home as a subject within the university, this may be a dedicated building, lab spaces or research environment. Based upon these observations, the idea of dedicated spaces in a largely technical discipline were addressed with results revealing most departments housed between one and four forensic-specific laboratories, each holding between 24 and 64 computers. Four respondents stated their laboratories were solely dedicated towards computer forensic students, while others identified specialist equipment was available in laboratories which may be utilised by other programmes across their institutions.

Furthermore, three respondents stated there was 24/7 access to labs available. Reflecting on the lack of round-the-clock access and dedicated spaces, respondents were asked how often spaces were used for lectures and practicals, and how often they were free for private study based on approximations per week. Table 5.2 shows there to be a reasonable number of hours per week when students can use the facilities for their own studies.

Lab time for lectures/practicals	Free for student private study time
4	30
8	12
20	20
20	25
20	30
38	130*
42	120

* per lab (incl. weekends and evenings)

Table 5.2 – Access time in hours for laboratories acknowledged by respondents

However, the true extent which students can use labs for these purposes will be largely dependent on their own weekly teaching schedule and use of the spaces for other classes. The highest amount of free time noted by one individual is 130 hours per lab, where there are three labs with forensic specialist equipment.

[14] Websites exist such as, Save the Student (2019) which helps students calculate the hourly cost of a course based on their UK university, course subject area, tuition fees and weekly contact hours.

The respondent notes that this includes evenings and weekends. It is also plausible that the respondent who notes 120 hours may have included weekends and evenings in their calculations, as the institution does have constant access for the space, as well as the four labs available for forensic specialist use.

Two participants stated that their students had problems gaining access, mainly due to the lack of vacant time during academic tutorial hours (e.g. 9-6 working period) and the busy nature of computing workspaces. Responses came from two individuals, where laboratory access could be said as opposite ends of the spectrum. One with multiple forensic specialist access labs and constant access available and, the other with only one lab available with specialist equipment and no 24/7 access. The two HEIs were similar in the sense that other departments/non-computer forensic programmes were able to book the dedicated space.

Those who noted issues reported that solutions were found by creating a themed lab (e.g. games, robotics etc.), booking extra unmanned lab time (i.e. specific lab access linked to modules or programmes with no lecturer present), and development of cloud-based virtual environments for further access. Those who found no issues with access to laboratories noted that extended access hours had been provided during term time with others maintaining 24-hour electronic access to the building.

This is something which has been set in place at CCCU for several years and alleviates some of the pressures and difficulties in providing and maintaining a dedicated space for digital forensics within a HEI. However, what the author and colleagues at CCCU have noticed is the negativity of students when there are enforced university closures such as holidays (e.g. Christmas and Easter). In recent years, these closures have included the building for computing where students have consequently noted their discontent toward these closures some feeling disadvantaged during these assessment periods. Student expectations may be managed in this scenario and closures are advertised long in advance. Furthermore, academics have initiated assessments which can be completed at home. Although, students have continued to find reason to grumble at the lack of access in these time periods; a potential weakness of providing 24/7 access in term time yet being unable to avoid university lockdowns.

When a makerspace was introduced at CCCU students who started studying without a dedicated space recognised how the room made improvements to their overall sense of belonging and engagement. Though, the benefits of this space once again becomes the norm to fresh students who may see this as a pre-existing space, where the future could see this add to the continuous demands for further resources and spaces.

5.1.3 Specialist Equipment and Tools

The necessity to keep up-to-date with tools, techniques and trends imposes several challenges in terms of both student expectations and monetary funds. Of those surveyed, three respondents stated their hardware was updated once every three years, with others updating every one to two years. Software on the other hand, was updated on a yearly basis as identified by 5 individuals, most likely due to licensing.

Responses were collected in January of 2015 having been distributed in 2014. At the time 2014 was the most popular responses for when hardware had been updated followed by 2013 (Figure 5.1). One respondent noted that hardware had not been updated since 2012 where the institution had one forensic specialist laboratory operating Windows 7. It is likely that institutions have since updated hardware and more so software available (if not only due to consequent versions).

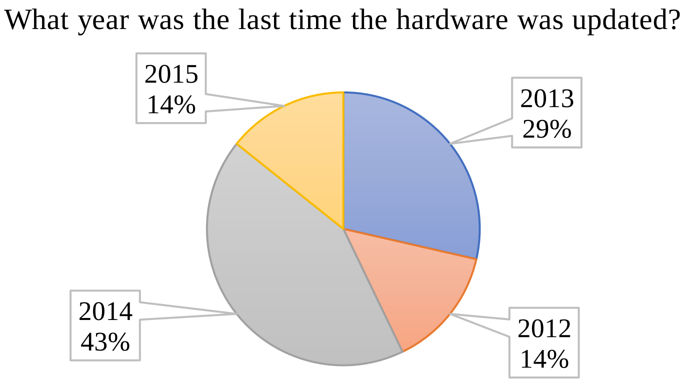


Figure 5.1 – Year of last update to hardware acknowledged by respondents

Individuals noted use of various Operating Systems, often where multiple were available including Windows 7, Ubuntu, and Kali. Two individuals referred to 'Various' and 'Any' as responses, this may suggest that as a department they house a plethora of bootable disk images for students to make use of. Respondents were asked for computer specifications of forensic laboratories, where the majority housed computers with i7 processors and 500GB storage capacity. One respondent was unable to answer the specification questions, however, Table 5.3 demonstrates the responses sought ordered by ascending HDD capacity.

Computer Specifications			
CPU	RAM	HDD Capacity	Number of Hard Drives
Intel Core2 Quad 2.8GHz	4GB	500GB	2
-	12GB	500GB	-
i7	32GB	500GB	1
Intel i7	6GB	1TB	1
i7 5960x	64GB	RAID 10 2TB, + 256GB SSD	6
Various	8mb	Various	Various

Table 5.3 – Computer specifications acknowledged by respondents

Of the six individuals who responded all note that there is a dedicated separate network for forensic purposes. Internet access was available on some networked laboratories, while one person noted that there was no internet access, and another noted that access was only granted for updates controlled via private NAT and firewall.

Several digital forensic hardware devices and software/license products were listed in two separate questions. Hardware devices included fundamental and key devices to following procedures of basic bit-for-bit copying and analysis such as, write blockers, and forensic kits from proprietary digital forensic tool providers. Figure 5.2 shows the results from all seven respondents and shows that write blockers, forensic duplicators, faraday bags/cages along with XRY equipment were available at the majority of institutions.

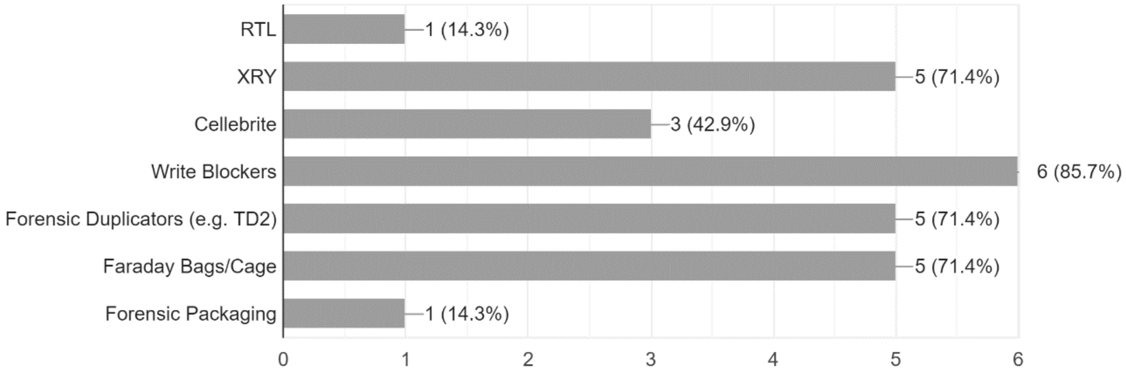


Figure 5.2 – Digital Forensic hardware devices acknowledged by respondents

For software/licensed products questionnaire respondents were provided with a range of tools; where, individuals noted utilisation of popular tools used within the digital forensics industry such as EnCase, FTK, Autopsy, Kali Linux, NetAnalysis and others, many of which were free and open source. Figure 5.3 demonstrates the tools which were most popular among HEIs who responded; these were EnCase, FTK and Sleuth Kit/Autopsy.

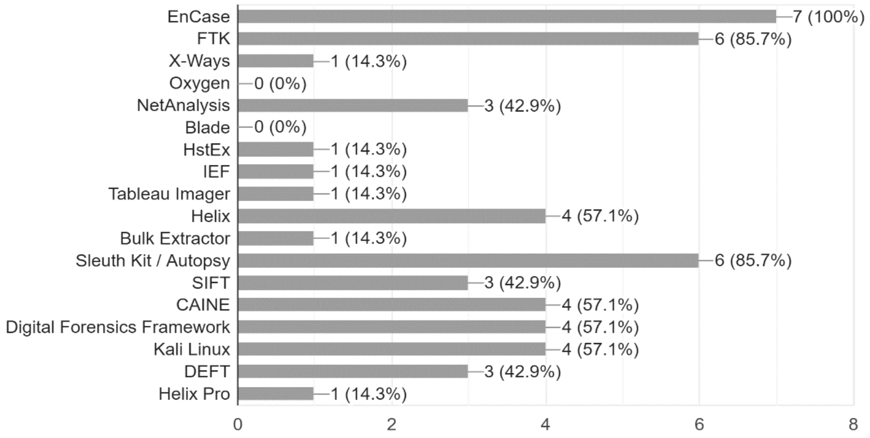


Figure 5.3 – Digital Forensic software/licensed products acknowledged by respondents

A discussion with one academic interviewee, although not exclusive to the academic institution, noted that "the degree programme is one [they] spend the most money on within their school because it is not cost efficient". They recollect how they have to "spend a lot of money on more powerful equipment, on licenses for software, on buying [devices] from [places like] eBay that you can use to give to students [to examine]. [So] it might be cost effective, but it is more costly than computer science for example"[15]. When asked how they felt about the problem continuing in academia and whether there was potential for the problem of cost being too much for institutions, the respondents expressed 'yes'. They noted that it was a matter of strategy in the current climate for the course and it was continuing due to its alignment with thematic areas introduced across the university.

5.1.4 Accreditation

Vendor accreditation within any subject is a point for debate. Accreditations often raise questions as well as potential positives and implications they provide to a programme such as, how much a course must adhere to guidance and weightings of topics, or inclusion of specifics such as examinations. Hence, they can often affect the programme design. Of those who responded to this question within the questionnaire, which were six individuals, four noted they provided accreditations from software vendors including ACE (two), EnCase (two) and XRY (one)[16].

This question was specifically aimed at vendor accreditations and identifying whether courses integrate specialist product accreditations and training into course design.

The questionnaire also looked to establish how many staff within each HEI had previous commercial experience in digital forensics. This was used as a measure to determine if there may be a lack of subject knowledge across the discipline within higher education. Academics who self-identified commercial experience, noted a maximum of three people in a department, with some having what they identified as no commercial experience.

Although a minority of respondents from the community, this preliminary study included seven participants from seven different institutions, where there are just over 30 courses across the UK offering undergraduate programs in courses relating to digital forensics. Therefore, although a small number of respondents, they are representative of just shy of a quarter of institutions across the UK. If this is indicative of the whole community, it could be argued that this demonstrates a lack in subject knowledge from a professional viewpoint, depriving students of key industry insights. This is, however, dependent on each academics'

[15] Technological devices often range from standard computers to dedicated computers and devices for forensic investigations in order to practically examine and analyse data in for example, scenario-based investigations.

[16] There was more than one response from a participant.

perception of commercial experience. Some could consider this to be sought through several routes, other than working in the professional environment, for example: working with and training law enforcement/security services and industry partners.

5.1.5 Observations: Computer Science, Computing and Digital Forensics

Respondents in the questionnaire were asked for any other comments which they felt would be important in this study, just one individual responded. Commenting their belief that "placing a forensics course in a computer science department is the reason many fail as they produce computer scientist not forensic experts and the gap is vast!" This is very interesting as most courses provided at Bachelor's level in the UK sit in computing departments. Further, it was noted in the literature review (chapter 2) both digital forensic and a selected number of computer science programmes were analysed showing that digital forensic courses are often driven by topics included in computer science programmes, while highlighting specific forensic modules to focus on broader elements such as the collection, preservation, acquisition, examination and analytics, presenting and reporting of evidence. Where for many courses it may be suggested that digital forensic and cyber security courses have emerged as an addition to existing computer science or computing programmes originally on offer due to funding and attractiveness.

Where fruition of digital forensic courses have developed from computer science courses, there are questions surrounding the delivery of programmes which can be classified as digital forensics. For example, should a digital forensic course with only one or two forensic modules be classified as computer science. Works discussed in section 3.2.3 are making attempts at defining what constitutes a course in digital forensics and cyber security and what is expected of programmes and outcomes for graduates and employers, however, interviews with academics show differing views. Again, adding to the uncertainty behind digital forensics as an academic discipline, discussed in section 3.1.

One interviewee along with other academics highlights how fundamental skills in computing are paramount to a digital forensic investigator's ability to conduct investigations along with the principles of forensics. The academic is of the view that a course which is more computer science with "say two modules a year in forensics" is perfectly valid. Furthermore, the academic describes that they are still happy for students to be learning mathematics, as computer science relies on a mathematical underpinning also described by Ryan and Shpantzer (no date). Though the academics interviewed identify that they do very little mathematics on their courses, where it is often "some really simple stuff". This may be due to its untrendy nature, which one academic acknowledges "that whenever mathematics is mentioned in a classroom setting half the class switch off". While mathematics is a core element to computer science the scale of learning may depend on both the course and later their career. For example, areas of machine learning and artificial intelligence will undoubtedly require statistics and vector mathematics, yet a programmer may only need to know some basic algebra.

Other academics stated they feel that a computer science course with elements of digital forensics is not always fruitful and does not define a digital forensic degree. Though as one respondent vocalises, the design of a course cannot solely be that of forensics as this would produce a highly effective graduate in one or two areas of the discipline and the skills and abilities they have obtained may only last a few years with the development and pace of technological advances. They acknowledge that "modules such as databases, all those that deal with raw data, operating systems and programming … are all important in understanding how the computer works and forensic tasks" leading to far greater depth and breadth of knowledge, skills and abilities for further application within digital forensics as technology advances. This is considered more closely in continuing chapters where discussions with academics, graduates and professionals highlight the requirements expected initially in industry, as well as thoughts and experiences with digital forensic degree programmes.

5.2 Academic Discussion on Digital Forensics as a Discipline and Lack of Frameworks

With the literature having shown uncertainty on the delivery of digital forensic courses in higher education and the placement of the discipline as an academic discipline, academic interviewees were asked to consider their experiences of these issues. Discussions with one academic led to questioning why the discipline has had troubles defining itself in the past as an academic discipline, where the academic felt that "because we [the subject] sit between two or three disciplines … forensic science, computer science and law … [that we] are trying to bring [all] those in". The academic mentioned that the academic discipline should not necessarily feel they must tie in all three areas, as digital forensics is a science of its own. They give the example of initial jobs within the discipline seen in police departments requiring degree programme to incorporate law as a key essential. Nowadays, they argue that this does not have to be the case due to the number of jobs available in areas of digital forensics such as e-Discovery and financial business. Conducting a quick job search for 'digital forensics' or 'computer forensics' on well-known advertising platforms results in fewer job advertisements for law enforcement or governmental roles, but those more akin to a corporate environment; supporting the academics claim. This may also suggest reasons why review in chapter 2 saw fewer course module naming conventions dedicated to legislation. Materials, content and programmes can therefore often be aligned for roles in consultancies and/or private sector companies conducting digital forensics and cyber security investigations. Although, the respondent believes some of the issues still lie in defining the subject, and that it is “a matter of identity” which they express the subject still lacks.

While “there isn’t a national curriculum”, all academics interviewed agreed that a strict curriculum would not work for the subject and there needed to be a level of flexibility in any framework or certification. Academic interviewees were asked why they felt there was a lack of framework and whether new standards could be successful. One academic recognised that the diverse range of programmes and unknown quality can make it hard for an employer to know what knowledge and skills have been taught and learned during a course when employing graduates[17]. They provide the analogy of a student taking an A-Level in Mathematics where, the content of the syllabus is known; so, if the employer is “math orientated” they would know a student should have obtained certain knowledge and skills. The academic describes that criteria of this nature for digital forensics education, be it national or international, may “give me greater confidence, as an employer, and it would mean that I know they have done this and this; so, your training needs (from what I know about the job) are this, this and this”.

Interviewees were aware of new efforts such as those by UK’s GCHQ[18] for higher education establishments. However, the academics note it is not mandatory and they have “found problems in trying to abide by the conditions” which meant a lot of “additional work to meet the minimum set of requirements”; some only meeting provisional certification. Others felt that there were too many changes which had to be adhered to and could change the context of the course and have not progressed[19] with any certification. This broad spectrum of thoughts leads to several questions on whether the achievement is successful in today’s educational environment (particularly with the differentiation of Universities in leagues). This is something which many of the respondents did not wish to comment on, however, with one respondent this did bring to discussion the position of post-92 universities and those belonging to the Russell Group. The experience at every university is important, however, differs across establishments. A lecturer having worked at both post-92 and Russell Group universities notes that this in itself is a much wider argument and something which needs to be considered further within digital forensics in academia. One academic also presented the feeling that not all courses need to be accredited and that it does not always add value. Accreditation and certification professionally within digital forensics have been a big debate among professionals and regulators (Beckett and Slay, 2011; Irons and Konstadopoulou, 2014; Sommer, 2018), and seemingly new standards within cyber security education advising on digital forensics may also

[17] GCHQ at the time of interviewing, and now organised by the NCSC, a part of GCHQ. This was again something which was highlighted in chapters 2 and 3 when current UK HE programmes, and existing literature were reviewed.

[18] Discussed in section 3.2.3 and section F.1 in Appendix F.

[19] At the time of the interviews (2017).

provide much wider debate and opinion particularly when, at the time of writing, there is little evidence of benefits of certification of this type.

5.3 Development of Scenarios and Forensic Images and Assessment Materials for Teaching and Learning within the Discipline

Since the incarnation of digital forensics into education, there have been many challenges associated with its delivery as aforementioned in the above chapter. What has particularly been a challenge in most, if not all, instances of digital forensics training and education is the tough time educators and trainers have in providing real-life and practical examples and assessments. This is exacerbated by the often unsuitability of data which exists in a real-life crime within the teaching space.

Literature suggest that "the lack of readily available data sets has … been problematic" (Garfinkel *et al.*, 2009), though banks of available disk images/case studies can be found through a number of individuals and organisations online, albeit outdated (Robinson, 2015; National Institute of Justice, 2016; Digital Corpora, 2017). The sparse recreation of datasets indicates the irreplicable nature of large digital forensic cases in education.

Society's reliance on technology has given rise to a mass of data, be it cloud based storage, disk drives, data centres, network packets or malicious attacks which in turn may be of evidential value in all walks of criminal, civil and corporate investigations. The likelihood of a digital device not being used in crime nowadays is slim. In the past it would have been unusual for professionals to have nearing twenty devices to examine for one case; this is now more than likely based on data extraction statistics[20] such as, Kent Police with 2,594 devices in 2016 and the Metropolitan Police Service having extracted data from 46,400 devices in the same year, as reported by a Freedom of Information Request by Big Brother Watch (2017, p. 21). Previous official statistics demonstrated that by 2014/15 the volume of devices examined by the Metropolitan Police, the largest police force in the UK, alone was at a staggering 38,622, though a slight decline on the previous two years (Metropolitan Police Procurement Services, 2015). The London Metropolitan Police Service alone admit to contracting fifteen "digital Forensic Service Provider (FSP)" to support the work of their internal Digital, Cyber and Communications Forensics Unit (Metropolitan Police Procurement Services, 2015). Stating that "[e]ighty five percent" of "atypical" devices which are of a nature where password protection and/or encryption has been used will usually be outsourced to one of their external FSPs (Metropolitan Police Procurement Services, 2015).

[20] Statistics show the number of devices data has been extracted from across 2013 to 2016 (Big Brother Watch, 2017).

So far a decrease in the backlog to digital investigations has been trivial with the method of triaging devices (Parsonage, 2009, pp. 12–13). An initial elimination phase using tools which can readily extract data and facilitate the rapid review of potential sources of evidence in order to prioritise the digital media for further analysis based upon multiple factors and may reduce the time taken during an investigation. James and Gladyshev (2013a, p. 148) undertook a study involving digital investigators to discover whether methods such as triaging are appropriate and acceptable to aid decision making on removal of the examination of exhibits in investigations. They state that the law enforcement involved in the study "was nearing 3 years" backlog with weekly additional exhibits and investigations. With the new age of Internet connected devices, the volumes of data and number of devices are inevitably going to increase over the coming years for digital investigators, once again. Where such evolution may continue to prove difficult adding to the complexities and improvements to processes, and the backlog may continue to increase.

These higher number of devices are undoubtedly irreplicable in the development of course materials within education meaning it is implausible and impractical to provide students with a life-like case containing for example, ten devices. While students need to be presented with life-like examples, balance is required due to time needed for teaching, learning, and researching as well as assessment and evaluation. Where the key essentials are the fundamental knowledge and competences they require. Additionally, training and educational programmes must consider the notion that they are not there to provide a platform for criminality and there is a fine line drawn where learners must be able to in some essences think like a criminal to catch them but must always remain ethical. Academics must be cautious of the materials that are presented to students; for example, the use of indecent images is unlawful, nor plausible or necessary in an educational context and, such an example would be swapped with other images. Though, an element of reality is invoked and required in these scenarios to replicate a "real" life case as much as possible. Academic respondents in this study have noted examples such as a range of animals in replacement for such images by way of desensitising materials. One academic epitomises this stating:

> "It is a lot of hard work. We have images of like 26GB in size which contain lots of different things and they need to be clean, so they don't give students stuff they shouldn't see, and they need to be enough to give students what they need to see."

Academics interviewed recognised that there were several forensic images and problem-based learning ideas within the academic domain including examples from groups such as, the "Digital Forensic Workshop … that are quite useful to give to students to play with." Academics also recognised that there are also images and or challenge-based learning ideas available from several cyber security and digital forensic challenges including some listed at Forensic Focus (no date). Though the academics recognise that the few images available are often outdated or technological advances require more materials. Acknowledged more so are the efforts and resources (time, technical and skills) required to create such scenarios which are often challenged by several demands and issues which academics have identified surrounding the delivery and development of programmes; including:

- dedicated laboratory costs and hardware (continuous need to update);
- license fees for industry specific tools (discounted, although still expensive);
- potential to isolate a network (dedicated resources required);
- a multitude of digital devices with evidential and non-evidential data (needed for a wide range of investigative devices);
- subject knowledge gathering and staff training costs/wages;
- small academic community and a lack of willingness to share content;
- limited number of case studies available; real-life case studies inaccessible due to sensitive nature etc.; and,
- time costs associated with material creation and development of diverse innovative tests/practicals to accompany scenarios.

Problems with the creation of scenarios have been reiterated by professionals who use the well-known digital forensic forum service, Forensic Focus, in discussion threads dating back to as early as 2013. An example of this is a third-year student from Leeds Metropolitan University who was looking for a willing "sponsor" to:

> "create an evidence image of anything, laptop/hdd/mobile that has say been seized in a criminal investigation. And then set a series of targets and goals that [the student] would need to achieve by examining this piece of evidence. Sort of like if [the student] was an employee of a forensics company and [they were given] a job."

One professional who goes by the name jaclaz (2013)[21] responded to the student that they "believe [the student] ha[s] hit the nail right on the head, there is a difficulty for a future investigator to work on "real" cases." While also discussing the risks that would go with a ""real" case exit[ing] the[] premises … [as] a serious violation of any number of Laws related to privacy and/or non-disclosure … and particularly if the case is a criminal one."

With others, such as a user who goes by the name of Adam10541 (2013)[21], noting the underestimation on behalf of the student surrounding the challenges even an experienced investigator or academic who

[21] Information from a discussion on Forensic Focus Forum dated 2013 (Forensic Focus, 2013).

regularly creates such images and materials would face for the time and effort that would go in to fabricating such an investigation.

> “You have actually drastically underestimated the amount of time this would take. To create a test image, then populate that image with say internet history, search terms, deleted files and various trace evidence, then to create a 'scenario' and come up with the pertinent questions for you would take quite a few hours. Not to mention that the person who created the image would first have to undertake the analysis themselves to confirm that the image actually does contain all the relevant data as needed.”

As Adam10541 (2013) eloquently reflects:

> “There are plenty of test images already available on the internet. Having attempted to create a test image … it’s not as easy to get the desired effect as you might think, and to put together something meaningful with all the needed elements would be quite time consuming.”

However, academics today continued to express that “there aren’t many new ones [datasets/images] being generated recently, which is a bit of an issue. Stuff that is being set as an assignment is, of course, being generated from scratch and that is a painful process and there are a lot of hours that go into that. It would be nice to have some sort of resource which is shared between universities [however,] good luck in getting that to work.”

Academics have noted that the demands of an academic or trainer often lead to scenarios being used year-on-year and easily becoming outdated. Although outdated, what can be said for these scenarios is they still provide students with elements of an investigation where they can apply theory to practice, developing their skills. Authors such as Lallie, Lawson and Day (2011) have previously noted shortcomings with particular reference to the reuse of materials within higher education studies and student “misdemeanour”. Lallie (2010) notes that some of these issues can be tackled through innovative ideas such as practical components to test student knowledge and further develop their analytical skills. This challenge is something that, as the curricula and discipline continues to evolve will need to be addressed. One interviewee in particular, notes how they tackle this by separating the assessments enough so that “they don’t find plagiarism[, and as] they are small classes and [they] have some great groups going through every year which is awesome and so those groups don’t appear to be people who are keen only to come to university to get a qualification, they are keen to learn.”

The troubling notion of these abovementioned challenges are that they are still issues seen today by academics within the disciplines. For most institutions a core of academic staff will “get together, think about some cases and somebody puts the whole thing together.” While it is apparent that within the community there is some willingness to exchange experiences and share materials this has yet to mature into a mutual digital forensic scenario curator or sharing platform.

Similar issues have been observed in training, where the researcher has had the chance to be involved in a project under the umbrella E.C.T.E.G. group and its partners to help develop scenarios which synchronise datasets used across training packages provided for Law Enforcement Officials. The project looks at implementing a large scenario which covers a multitude of data types and can be used with several analysis techniques, predominantly using open source tools. The idea behind the project is similarly based on challenges abovementioned e.g., the time-consuming nature of curating scenarios per course (for which there are eighteen training courses available through E.C.T.E.G. to date). The idea being to create a methodology for scenario curation and upgrades for a modular approach, based on experiences and challenges when developing and implementing data across several types of investigation and levels of training.

5.4 Summary

This chapter has reviewed resources (e.g. hardware, software, and staff) noted by several academics delivering digital forensic degree courses, where seven responses were gained. The data revealed that the resources across HEIs are vastly different with some institutions providing a sizeable number of laboratories and several with digital forensic specialist equipment, while others are provided with just one. The results also showed that there were issues across the HEIs such as access to laboratories out of teaching time and the expectations of students. Although, monetary costs associated with these courses were not identified digital forensic courses do present higher technical cost than a typical lecture-driven subject.

Other issues conversed include examples of a lack of staff with related professional experience, costly resources, and high expectations. Another of the greatest challenges identified affecting HEIs is the production of quality resources and case studies; a timely and extensive task which could see the need for an automated tool to create such activities and to greatly aid the learning process.

The next chapters look at viewpoints of several stakeholders captured in this study identifying expectations and experiences of individuals from academics to professionals, students to graduates and members of the general public.

6. Digital Forensics Education: Insight and Experiences from Academics, Students and Graduates

Introduction

As with any profession and associated degree programmes there are several stakeholders who are set to gain from graduates seeking employability and while this a positive for industry there are several initial expectations and perceptions which must be understood and managed throughout a degree programme. These are not restricted to the expectations and perceptions of potential students but also industry professionals and alumni. This chapter focuses on the views of three main target audiences of this study: academics, students and graduates. Figure 6.1 (below) demonstrates the relationship of these target audiences, identifying just a few selected influencers of each group. For example, initial student expectations of a course must be managed by academics through awareness, content design and delivery; however, these can also be managed using alumni who can contextualise a student's learning through their own previous experiences of a course applied with job practices, skills and requirements.

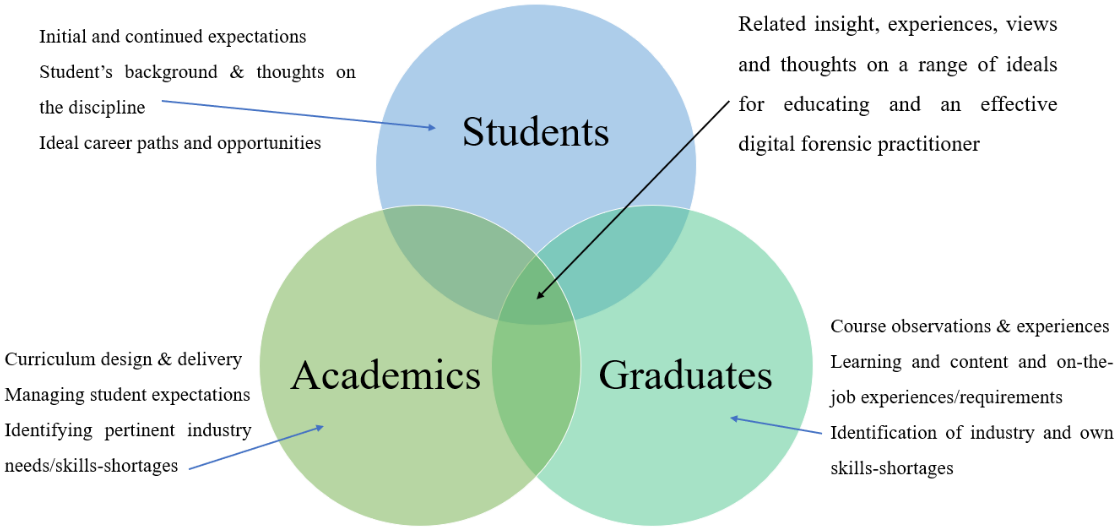

Initial and continued expectations
Student's background & thoughts on the discipline
Ideal career paths and opportunities
Students
Related insight, experiences, views and thoughts on a range of ideals for educating and an effective digital forensic practitioner
Curriculum design & delivery
Managing student expectations
Identifying pertinent industry needs/skills-shortages
Academics
Graduates
Course observations & experiences
Learning and content and on-the-job experiences/requirements
Identification of industry and own skills-shortages

Figure 6.1 – Academic, Graduate and Student Target Group Relationship

Due to their close connection with academia these target groups are bound together in this chapter focussing on understanding what ideally makes an effective digital forensic practitioner as well as the challenges which are faced with prior expectations, awareness and contextualisation of the discipline, future work and skillsets and a range of observations and experiences which highlight how the academic discipline needs to continue to grow and deliver. This chapter therefore considers the views, perceptions, and experiences of several participants from three main target groups presenting a range of themes across each stakeholder: academics, students, and graduates.

6.1 Recap on the Method

Within this chapter, questionnaires and semi-structured interviews were conducted. Participants were selected through convenience sampling where interviews were conducted with known individuals and a questionnaire spread via social networks and email as discussed in section 4.4 of the methodology. Interviews were conducted in a semi-structured fashion where pre-determined of open questions to prompt discussion were created allowing the researcher to explore themes and responses in more details. The information gained from these interviews and questionnaires were coded during thematic analysis, as discussed in section 4.4.7. Analysis of these qualitative data examined and looked at identifying and interpreting common and recurrent themes, across the target groups within this study.

Furthermore, to capture and understand perceptions, ideas, and experiences of students, workshops containing a questionnaire were conducted and contained discussions and a post-mortem of the results. Students studying level four in digital forensics and cyber security were considered at two institutions. This level of study was chosen due to the comparability of fresher students to graduates and, further for their ability to recall their original thoughts on the fields with potentially less bias than those who have studied the subject for several years.

6.1.1 Rationale and Themes of Questions for Academics, Graduates and Students

Based on the research questions defined in section 1.1 and previous research discussed in chapters 2 and 3, several questions were determined for the interviews and questionnaires with all stakeholders. This section discusses the general areas of the questions posed, their importance, focus and reasons behind their inclusion[22]. Questions were used to promote discussions in areas such as learning, training, topics, skillsets, and challenges.

[22] In total there were several questions which were used to guide the interviews, and discussions were semi-structured and guided by views and experiences of interviewees.

This section breaks down the themes of questions targeted to the three main stakeholders discussed in this chapter, namely academics, graduates, and students before discussing the rationale of these themes.

Stakeholder Group	**Question Themes**[23]
Academics	- general experiences in designing and developing courses in the field - resourcing within digital forensics education - challenges experienced in producing and delivering a course in digital forensics - observed best practices for learning digital forensics - balancing theory and practice - fulfilling industry needs/demands and keeping pace with the field - thoughts on skills-shortages and approaches addressed in education - thoughts on existing frameworks for cyber security, and by extension digital forensics - balancing training and education
Graduates	- recollecting learning experiences - choosing the course and their initial thoughts/expectations - studies preparation for industry - interesting/important subjects learned and their application - application of theory, practice, and assessments - challenges, improvements, and limitations - own thoughts on their career trajectory - own learning styles - industry experiences and application of their learning - skills-shortages and industry/educations striving to keep pace - frameworks for digital forensics
Students	- interests in doing a course in digital forensics and/or cyber security - employment/career progression and subject interests - thoughts on public awareness of digital forensics/cyber security - skills-shortages and industry/educations striving to keep pace - skills of a graduate for employability - own learning styles - importance of education, training, and experience - initial expectations and reality/improvement of courses - thoughts on subjects such a degree should include - improvements to education to support employability

[23] Example questions can be found in Appendix A - A.1—A.3 and A.5.

The rationale behind these themes were relevant to the research aim to assess perceptions, views, and experiences of several key stakeholders who are involved or have experienced education and training in digital forensics. Existing research, discussed in chapters 2 and 3, have shown there are several challenges presented within the field of digital forensics, and particularly issues of resourcing and practical learning within education settings. Researchers have rarely considered the expectations of students and graduates, how to manage them, the effects of challenges experienced by academics and trainers on the employability of graduates, or on the wider and potential skills-shortages within the discipline. Furthermore, existing research lacks thematic relationships among stakeholders. For example, the thoughts of professionals on graduate skills and abilities, graduate thoughts on their learning and employability, topical interests of students and their expectations at early stages of a course, and academic responsibilities, experiences and challenges combined. Based on the lack of narrative, lack of attention drawn to and comparison of challenges, expectations, development, design and so on, this study identifies common themes among participant responses to questions themed above and addresses any relationships throughout the next few chapters.

6.2 Participant Information

The aim of this section is to highlight and describe the characteristics of the academics, graduates and students surveyed or interviewed within this study (n=55). Table 6.1(below) displays the role, gender, years' experience, and site of interview for participants across three stakeholder groups within this study, namely academics and graduates in this chapter[24]. There were particularly varying years' experience across these participants.

[24] Detailed demographics (including all characteristics such as, gender, work and educational experience and years' experience) can be found in Tables B.1.1 to Table B.3.2 in Appendix B.

Participants (p) – Interviews

Target Group	ID	Occupation or Industry	Gender	Years' Experience*	Previous Role** Years' Experience	Interview Duration and Site
Academics/ Trainers (A)	A1	Senior Lecturer	m	2.5 years	Professional – 12 years	1 hour 10 mins - R-Campus
	A2	Principal Fellow	m	5 years	Academic – 13 years	1 hour 40 mins - I-Campus
	A3	Principal Lecturer	f	2 years	Academic – 10 years	55 mins - R-Campus
	A4	Head of School	m	4.5 years	Academic – 17.5 years	1 hour 10 mins - I-Campus
	A5	Professor	m	26 years	NA	20 mins - Conference
	A6	Associate Professor	m	3 years	Academic – 7 years	1 hour 5 mins - I-Campus
	A7	Programme Director	m	10 years	Professional – 15 years	1 hour 10 mins - R-Campus
	A8	Senior Lecturer	m	2 years	Total years' experience = 9	20 mins - I-Campus
	A9	Lecturer	m	2 years	Professional – 9.5 years	Email
Graduates (G)	G1	Corporate	m	2.5 years	-	1 hour - R-Campus
	G2	Public Sector	m	1.5 years	Corporate – 3 months	1 hour 10 mins - Business
	G3	Public Sector	m	1 year	Public Sector – 1 year	40 mins - Business
	G4	Public Sector	m	1 year	-	1 hour 20 mins - Business
	G5	Public Sector	m	2 years	-	1 hour 40 mins - Coffee Shop
	G6	Public Sector	m	1.5 years	Public Sector – 1 year	1 hour - Coffee Shop
	G7	Public Sector	f	1 month	Public Sector – 6 months	1 hour - Coffee Shop

R- = Researcher I- = Interviewee
*Current Role **Previous Roles Combined

Table 6.1 – Academic and Graduate Interview Participants, Locations and Duration

Academics

A total of nine academics were interviewed with job roles ranging from Deans and Heads of Schools to Professors and Lecturers across several HEIs as well as law enforcement education and training. Of the academics interviewed only one identified as female. It should be noted that this is not representative of the female population within academia, however, there is a distinct and disparate smaller proportion of women in academic computer science and engineering (formerly discussed within Chapter 4).

A range of years' experience were held among interviewees, some holding long-lasting careers in academia (e.g. two participants holding over 20 years) while others held lengthy careers professionally before moving across to academia to apply their on-the-job experiences to education. All academics interviewed held 10 years' experience or more when combining their academic and professional careers. Full demographics for these participants can be found in Table B.1.1 – Appendix B.

As individuals progress through their careers, be it academia or professionally, they transfer a range of educational, professional, social and cultural characteristics from past and new experiences. These personal experiences and characteristics are differentiators which can provide varying views, ideas and abilities among interviewees. For example, an individual with greater lengths of professional experience in digital forensics views and ideals will often be subjective to the job roles they have held and training they have received and may not possess as much experience for teaching or training.

Academics were asked several questions to determine their own interests, experiences and views on what makes an effective digital forensics graduate, an effective curriculum and teaching and identification of shortcomings and hurdles in providing education for the skills sought within the discipline. Questions were not used to focus on the technical side of computing and looked for qualitative results of their general experiences and application of real-world practice or academic practice to the subject. Themes focused across questions on experience and requirements, topics of interest, learning and development, industry expectations, student expectations and more[25].

Graduates

A total of seven graduates were interviewed where only one individual identified as female. Graduates were asked to complete a pre-interview information form which sought demographic data regarding the individuals' employment, experience, and qualifications/accreditations. The data (Table B.2.1 – Appendix B) shows that the seven computer forensics graduates are at relatively early years of their careers with all being at the time of writing within four years of having graduated. While a call for participants was advertised through the alumni relations team at Canterbury Christ Church University to alumni from the "Forensic Computing" course (as it was named at the time), this study found that recent graduates known to the researcher were those willing to participate. It may be argued that this section lacks representation of all computer forensic graduates from CCCU and furthermore representation from graduates from other institutions, however, it should be kept in mind that results captured are from graduates who have been able to gain relevant experience in the few years they have been employed. Another positive being all graduates interviewed were previously enrolled on the same course (Forensic Computing) albeit across multiple years. It should be noted that subjectivity at this stage is apparent with all participants in this study and their views

[25] Example questions are outlined in section A.2 – Appendix A.

and experiences will not only be based upon previous education but also current and previous job roles and skills or practices required.

What was interesting to note were how some graduates identified challenges in entering in to such a role in Law Enforcement after graduating where two graduates noted they chose to volunteer within the sector for a substantial period before they were able to obtain full-time employment within the public-sector roles as a civilian. They recognised this was largely due to their lack of experience within the sector, which was required in numerous roles and can be seen of many public-sector job advertisements to this day. Another noted they worked in the private sector first and moved across to the public-sector when a role became available. All but one graduate who responded to the interview call worked within a role in law enforcement (e.g., Digital Forensic Analyst or similar), albeit with different levels of experience based on years in the role and previous occupations and training. Those in law enforcement had obtained several weeks of training for specific tools used on-the-job.

Graduates were asked a range of questions which looked at similar themes to academics, professionals, and students. Questions[26] focused on initial course expectations, course delivery, beneficial course content as well as missing components through to preparation for industry, industry experiences and skills requirements and more.

Students

In total 39 students took part in the workshops delivered across two institutions (n=37 in supervised workshops; n=2 in a later lab class). Participants identified from varying backgrounds, with over 80 percent of the students identifying as male. While students were asked for their age and gender concerns were raised by a minority of students that they may be identified by these characteristics (e.g., if there was only one male in the class between 18 and 24). To satisfy these concerns and protect the identity of participants ages have been eliminated from this target group (see Table B.3.2 – Appendix B) and described as a group where, the lowest age range was between 18-24 and, the highest 55-65 with one respondent noting they were doing the course out of “interest”. Due to the timetabling of workshops, some included computing students, these have been eliminated from the demographics of students and considered separately in Appendix D – 0. Demographic data (Table B.3.2 – Appendix B) shows that most students (79.5 percent) did not have previous experience (i.e., work, educational work experience or placements) in the IT sector.

[26] Selected example questions are outlined in section A.3 – Appendix A.

Student workshops included a questionnaire[27] and post-mortem analysis of the responses in lab classes based at each HEI. Students were asked to consider and identify what their reasons for studying the course were, their expectations, career ideals, forms of learning as well as more specific questions relating to course coverage and content they believe should be included in a digital forensics and/or cyber security course.

6.3 Thematic Views from Academics, Graduates and Students

From the three stakeholders considered in this chapter, there were common themes found among responses:

- meeting, managing and balancing expectations;
- issues with awareness and contextualisation;
- stakeholder collaboration; and,
- knowledge, skills, abilities/competences.

6.3.1 A Reality of Meeting, Managing and Balancing Expectations

Meeting and managing expectations is a high priority across HE and involves several stakeholders (e.g., academics, students, university staff, employers, and industry alike). The value of defining and shaping expectations and perceptions of HE as well as digital forensics were points noted by academic interviewees. Points raised ranged from a students' initial perspective of the course and/or disciplines through to the way courses are structured and delivered, what content is delivered and why along with possibilities for placements. Managing student expectations and perceptions is central to their engagement and learning, particularly in feedback of the perceived worth of their own degree. Some may argue that meeting student expectations is much higher pressure with the current elevated HE costs for students, and while student expectations must be considered, reflections should be made towards the validity of these outlooks and their reality.

Academic interviewees highlight that student initial perceptions are not always realistic to the programme, expressing that, in some cases, the impact of the media and dramatic licence on digital forensics and cyber security are still an issue affecting the perceptions of the subject on arrival at university open days. Many utterings of "tell[ing] them upfront … it is not like CSI; that is not real". The issue with dramatic licence in these cases are its portrayal of a complex and intrinsic subject with routes grounded across multiple disciplines including computer science to an unrealistic and in some cases a more simplistic role. Many media representations (e.g. film, television, news) 'replicate' a digital forensic or cyber security

[27] The questionnaire can be found in section A.5 – Appendix A.

professional whereby they harness an element of the truth but are often far away from the real-life role. Interviewees note that managing this perception is a priority which must be tackled at the beginning of the student's journey to ensure that the learning they achieve is principal in guiding the student's expectations for what they will learn and achieve on a course.

Though, it is not always a student's initial understanding of the discipline which can cause issues. One academic observes that some students, when they first arrive at university, do not understand what a file system is, they do not understand directory structures. The academic vocalises "It's incredible the last couple of years have been shocking to me", recognising that previous year's students were more aware, but in the last few years they have found students have less awareness of simple things. One example the academic gave the researcher was of students saying, "oh where has my file gone?" and as the lecturer they have to ask, "where did you save it". This is something the researcher has also observed during lab-based settings, where some first-year students struggle to extract/unzip a folder and are often unaware where they have saved their files. Ideally, these are simple things which would be expected of a potential computing undergraduate student before heading to university. This study highlights that with the introduction of computer science in secondary school education opposed to information technology (IT), these issues may be resolved for future cohorts.

6.3.1.1 Initial Awareness and Expectations

In order to cross examine expectations across the several target groups, for example: students and graduates, preconceptions of courses and attractiveness of such a discipline were considered. Both graduates and students were asked to express views focussing on their initial thoughts of the course, why they chose computer forensics/cyber security, thoughts of the disciplines prior to studying, as well as how their thoughts developed across the duration of their studies. Undoubtedly, expectations of a HEI and a course change throughout the degree time and are heightened by levels of stress, uncertainties, and through the influence of peers and associates.

Of the student voices collected in this research, expectations of HE and courses included awareness of being stressful and challenging yet providing the ability to gain knowledge of an in-depth and technical subject. Some expressed the feeling that lecturers would be like schoolteachers, although there would be need for more independent work which could be intense but interesting where "knowledge and support to achieve the degree" would be available. Some responses focused on the style of learning for example, "that the learning would be more flipped" and there would be "small, lab-based lecturers that were hands-on not just with practical work but also learning". More specific responses toward the discipline included one student who expressed how they expected the course to teach them "how to use the tools associated with Forensic computing, [but they] did not know much about the course … expecting less essays and more hands-on stuff". Further examples involved expectations of "high quality teaching to be made interesting and fun" and "lots of practical applications of computer security".

One graduate interviewed stated how the course/discipline was appealing because of the potential jobs and that they were "17/18 at the time and [they] had the wow hacking! cool! Mindset. Which [they said] is kind of a bit embarrassing to admit." The participant expands that it is embarrassing because "knowing what [they] know now about the course" there is more to it than that and different than what they expected. The participant was also asked if they felt their initial thoughts changed in anyway over the course. Describing that, yes, they felt the course "would be more focused on hacking, however, it was not [, this] did not bother [them] as [they] would still be learning very cool things … and enjoyed learning; its subtle differences and thinking about it over the three years." The participant also expressed that "the lack of focus on [hacking] was not detrimental in [their] career so far" noting that "it would have helped for network security … and pen testing", neither playing great contribution in their current role.

Student views of digital forensics and/or cyber security prior to starting the course were at times vague with some noting "it is interesting", "important", "positive" and "a growing field". While others noted how they had taken an interest beforehand or felt they were aware noting it as a hands-on highly experience driven but lucrative profession and an "important part of solving crimes" with many focussing on the idea of cyber security through examples such as, "you go to a company and assess their computer systems find problems and offer ways to patch them in the form of a report" and "my view was to provide security from hackers from compromising the Company IT systems or to prevent malware infections". One response highlighted "that it was something that affected everyone without them realizing" and another stating "that [the disciplines/issues] need[] to be taken in a more serious matter", somewhat highlighting the lack of awareness possessed by people. Other respondents were open about their lack of awareness; for example:

- "I was not aware of all the fields where it is applicable and also did not know about its implications and impact"
- "I had no idea what is was except criminals committing offences online"
- "Like a secret service (spy)"
- "forensics, I thought, was just the police force really"
- "didn't know much about them."

There were, however, some interesting responses to both expectations and views of the disciplines with one student in particular acknowledging how differing views among peers on why they chose such a course are noticeable, stating: “I was expecting the students on the course to have the same enthusiasm towards learning as me, turns out 90% picked the course because it sounded cool.” While one academic with over ten years’ experience noted how they would start by getting students to “look at cybercrime and try and define it” noting “that’s always fun as no one has ever managed that”. Furthermore, academics interviewed in this study noted experiencing higher dropout rates than liked of students in the first year. Some spoke of team discussions centred on reasons such as, students not knowing what they are letting themselves in for and the need to manage initial expectations and perceptions. This resonates with the examples provided with many students either unaware or attracted to the courses because of the interesting nature and job prospects. This arguably poses the question, is it any wonder the discipline has previously struggled to define itself as an academic discipline when a lack of awareness and understanding of expectations continues to be a recurring theme.

Authors such as Kinnunen *et al.* (2018, p. 202) identify there are higher dropout rates in computing related courses with reasons identified as “a loss of interest in the computing field and career” or “feelings of not belonging” where a different discipline may be more fruitful and “fulfilling”. These are often reasons which may be linked with a lack of awareness or differing initial expectations which are not met or managed. Some academics conversed that to manage these issues they started to provide practical sessions on open days where potential students can see small tasks as examples of what they would be doing on their course. At CCCU these are conducted at both open and applicant days for HE computing-related courses including digital forensics and cyber security. The researcher of this study has found these sessions are fruitful in raising awareness of the course deliverables and expectations, engaging both student and guardian of what such as discipline entails as well as wider HE expectations.

While others noted how they provide students with courses such as Codecademy (Codecademy, 2018) to complete before attending the university as a means to help engage applicants in coding concepts, data structures and so on. One academic revealed how staff at their HEI were concerned that if they made the first year less technical, as a mechanism to reduce the dropout rate, that in fact it would shift the problem to the second year. Recognising that there is also a problem with understanding why a student has dropped out and how the issue can be tackled, data obtained often expressing it is due to personal reasons. The academic notes dropout rates are:

> “an issue across computer sciences, but [they] do think it is an issue for specialist degree programmes because students have a vision about where they are going to end

> up, they have vision and expectation about what their degree programme is going to do to get them where they want to go and there may be a substantial mismatch between expectations and what they actually have to engage with."

Clearly, there may be several reasons for a student to consider dropping out so early on in a course, however, taking this idea into consideration students within this study were asked to identify if their expectations and views were similar to reality and met by their courses, elaborating on how they could be met further. While this question adds bias and subjectivity, it allows students to identify areas they felt improvements were necessary. Of the 39 students involved, more than half of the students felt their expectations were met or realistic (Table 6.2).

	University A		University B			
Expectations	Total n	(%)	Total n	(%)	Total n	(%)
Realistic and Met by Course						
Yes	9	(56.25)	14	(60.87)	23	(58.97)
No	5	(31.25)	2	(8.70)	7	(17.95)
Unsure	2	(12.50)	4	(17.39)	6	(15.38)
Module Dependent/Partly	0	(0.00)	3	(13.04)	3	(7.69)
Total	16	(100.0)	23	(100.0)	39	(100.0)

Table 6.2 – Students' View on Disciplines and Course Expectations

Pre-empting some negative responses (n=7), all students were asked to elaborate on how their expectations could be met further. Responses ranged from comments highlighting it was dependent on the module, more time with lecturers on a 1:1 basis and more time learning and with assessments. The need for more practical and field experience was the most mentioned ideal improvement (eight occasions), along with the need for more case studies and live demonstrations related to the work in industry (four occasions). One student expressed how "work placements from the first year even if it was 1 day per week, as similar to nursing degrees" would be useful. Supporting this, graduates interviewed noted that placements within industry would have been highly beneficial; one stating, "even a month or two in industry to see how things work would have been ideal … working [in industry] is very different to university."

What is interesting is how a student has associated the discipline of medicine with digital forensics. Section 2.4.1 discussed how education for mastering a medical occupation includes focus on students within the working environment as an asset to their learning. What this student suggests is plausible and could provide better theory-practice links within digital forensics where students can practically learn on-the-job while in education, akin to an apprenticeship scheme, which could provide benefits for both education and industry alike. Although, not well-evidenced in the literature, the author of this research argues that there are many similarities, relationships and comparisons which can be made with education and training in digital forensics and that of medicine; particularly when it comes to hands-on practicals and gaining experience where lessons can be learned. For technical, fast-moving and ever-changing disciplines like digital forensics and cyber security lengthier and integrated work placements in higher education could induce an environment aimed at producing effective forensic practitioners based on real-life theory-practice links. Arguments against this may be presented in the form that digital forensics is a security driven profession, where businesses may often be reluctant to take on students due to not only the expense but also the need for security provisions and expertise. While, to some extent this is true today, similar hurdles and reluctances could be argued within a medical setting (e.g., a student observing or helping to conduct an examination on a patient, the need for discretion, confidentiality, protection, counselling and more). This study therefore argues that digital forensics education should in the future look to adopt a similar approach to education in order to deliver effective forensic practitioners using lengthier workplace opportunities.

A claim by another student who felt that to meet their expectations “focusing the course modules more towards ones that an employer may look for in a graduate of this specific field” was necessary. Their response suggests they feel their course does not tackle topics and skills required of a professional and centres on the need for greater awareness. During course creation of most, if not all, academic degree programmes there will be input from industry professionals as a measure to ensure courses are covering relevant industry topics and skillsets. However, these viewpoints and expectations based on industry insight must be balanced. One academic states they “do not believe that a degree programme should be designed to meet a particular industry need as we [the academics] have to offset the breadth of material that students should be engaged with as well as the technical training they should be doing.” Contribution from industry can be as little as a meeting between several academics and industry professionals, a panel who look at the course structure and seek advice or requirements from professionals through to industry involvement in teaching weeks or as guest speakers. Academics are tasked with recognising the subjectivity of several professionals’ own experiences, specialisms and current roles or industry requirements and interactions based on wider specifics to deliver the most relevant and effective course content delivering the most pertinent topics and skills.

Some students focused on the want for more work specific to digital forensics and cyber security where they found the need for “less generic computing” and “programming/software development”. This is an interesting point, particularly as the two institutions run courses which are computer forensic and cyber security based. This is also contrasting to the views of academics and graduates who felt that these skills provided them with the underlying knowledge to be able to conduct digital forensics tasks, often graduates noting how their theoretical and programming skills provided them with their job opportunities or valued industry skills. Where graduates could recognise the need for fundamental computing in the first year of a course to cement their basic knowledge and address broad requirements and qualifications sought for university entry[28].

What is extremely interesting is how one student picked up on the need to "ensure[] everyone on the course [is] at the same level of knowledge leading to more efficient lectures where everyone was capable of doing anything", they felt "that some people including [themselves] could have done with a few sessions" which ensured this; arguably, this is what the first year[29] is most often used for and something this student may not recognise until moving into second-year studies. This juxtaposes some graduate comments which reflect how the first-year seemed too simplistic in areas, highlighting a range of personal learning paces, styles and experiences which academics must consider. Thus, this shines a light on the need for lecturers to manage expectations further, particularly making students aware of the course structure and why they are learning specific topics in a computer forensics and/or cyber security course. One student boldly claimed they felt their course was "definitely covering topics that [they] deem outside of the required study for a forensic practitioner in [the] first year." This centres back on the validity of student expectations and whether a student truly knows what is expected in the workplace/of practitioners and their awareness and ability to contextualise course offerings.

Discussions with several graduates from CCCU raised questions over first year studies at university being too entry level. This question grew to fruition when graduates discussed how they felt the "first year was a bit wasted". While also recognising the need to ensure all students have the basic knowledge to start the course. Comments included:

- "I did an A-Level in Computing … what I had learned was in the first year apart from Transfer and Trace[30], that was the only one I really had to learn for."
- the course "did not have much about forensics [and] it started off assuming someone wasn't trained in computer science or computing. I did an A-Level in computing and feel it was at a similar level, not a higher level."

To these graduates "the first year seemed at a lower level than [they] had anticipated, apart from the digital forensics modules … which was the only part of the year which [they] found particularly challenging and

[28] This led to discussions with some graduates regarding the need to change some university entry requirements.
[29] Level 4 = first year; Level 5 = second year; Level 6 = third/final year.
[30] Trace and Transfer is a module which covers Crime Scene Forensic Investigation.

the most interesting." One noted that "by the time you got to the second year you really got into the nitty gritty bit of it."

Another graduate noted progression of the course got harder as the course developed, particularly in subjects such as, networking:

> "It got harder as the course went on because it was more complex. Especially subjects like networking where I had done the basic subject at sixth form level and breezed through the first year but then suddenly it just leapt up in the second and third years and I had to catch up and I had not experienced that before. I think it was pretty steady through all three, the only thing that threw me was having to do the dissertation at the last year it was a completely different style of something which I had to do. I hadn't really encountered anything like it."

This question has been raised several times over the years in the news and across student forums (The Student Room, 2013; Seldon, 2017; Carmichael, 2019) where conceptually students seem to have a mixed view of which is harder, A-Levels or the first year of university. Addressing the difficulties such as students learning to manage their time and make the most out of a year which does not count towards their final grades. Graduates interviewed in this section are and were clearly exceptionally intelligent students and thrived in situations where they were challenged. Arguably, their interest to be a part of this study shows their willingness to make change. However, from the researcher's active research, i.e., presence and observations in first year teaching across modules in computing, academics must account for students who attend university with very different skills and attributes. The readiness for university in specific areas such as research, studying, writing, critical thinking, teamwork, management and so on is often lower than the researcher expected at their working institution. The researcher's opinion being there is a general sense of ineffective academic preparation at school level in preparing students for the next stage of education and for employment. Students do, however, recognise their lack of learning at lower levels in education to complete specific tasks relating to, for example, researching and writing skills become stressful at university and sometimes students are unable to contextualise these skills requirements within industry.

Authors such as, Salt, Lallie and Lawson (2011) note that managing unrealistic career plans and aspirations is something else which institutions providing digital forensics must tackle. One academic, when asked about skills-shortages in the industry, noted that managing aspirations for career growth is essential to student learning satisfaction; stating:

> "Students see digital forensics as being high-tech crime units. However, there is a lot of digital forensics in financial institutions and fraud departments. Students don't see that or apply for those roles. They all want the sexy jobs in the high-tech crime units."

Another reiterated this point highlighting that they felt a skills-shortage in digital forensics in policing is related to a money shortage where they are not able to cope with the workload they have now. The academic was unsure if they "would say there is a skills-shortage in forensics" but they would in cyber security. Recognising how roughly half their students go the forensics route and the other half go the security route. Noting how in more recent years "there has been a large number of people graduating from forensic degree programmes but then there have been a large number of places. Corporate forensics is something which has grown quite dramatically, so law firms look for various people."

To find out what career opportunities the sample of students in this study would be looking for, they were asked several questions pertaining to job roles and sectors, wages and specialist topics. Students were asked to consider their main reason for choosing digital forensics and/or cyber security, where results showed 30.8 percent felt their choice was linked to their interest in intelligence, following by 17.9 percent by their interests in computer science and ICT (Figure 6.2).

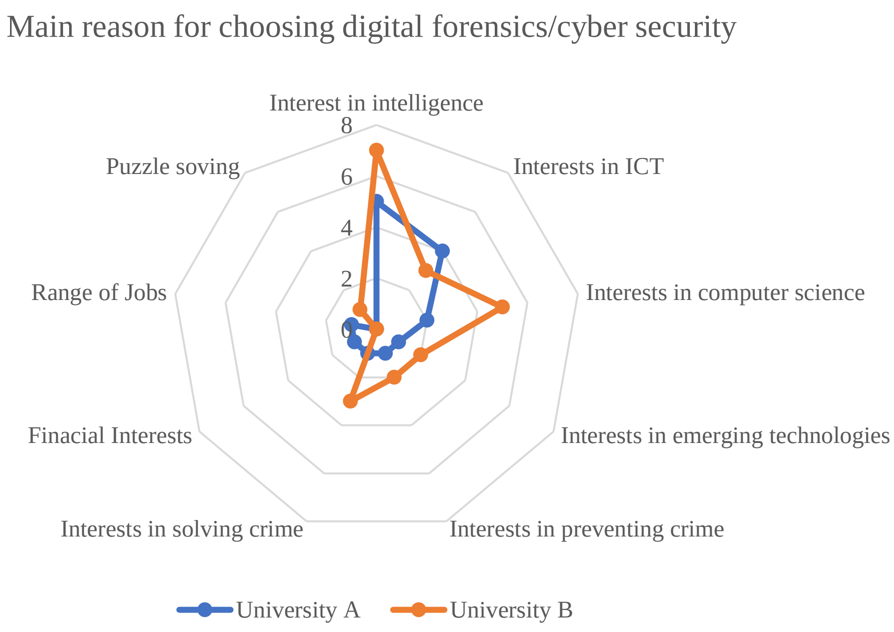


Figure 6.2 – Students' Main Reason for Choosing Digital Forensics/Cyber Security

While results ascertain that, of the 39 students, there was an equal division between those seeking a profession in public and private sectors with a strong consensus towards a career in cyber security (Figure 6.3[31]). Other students noted they were unsure or, were open to either public sector or private industry roles.

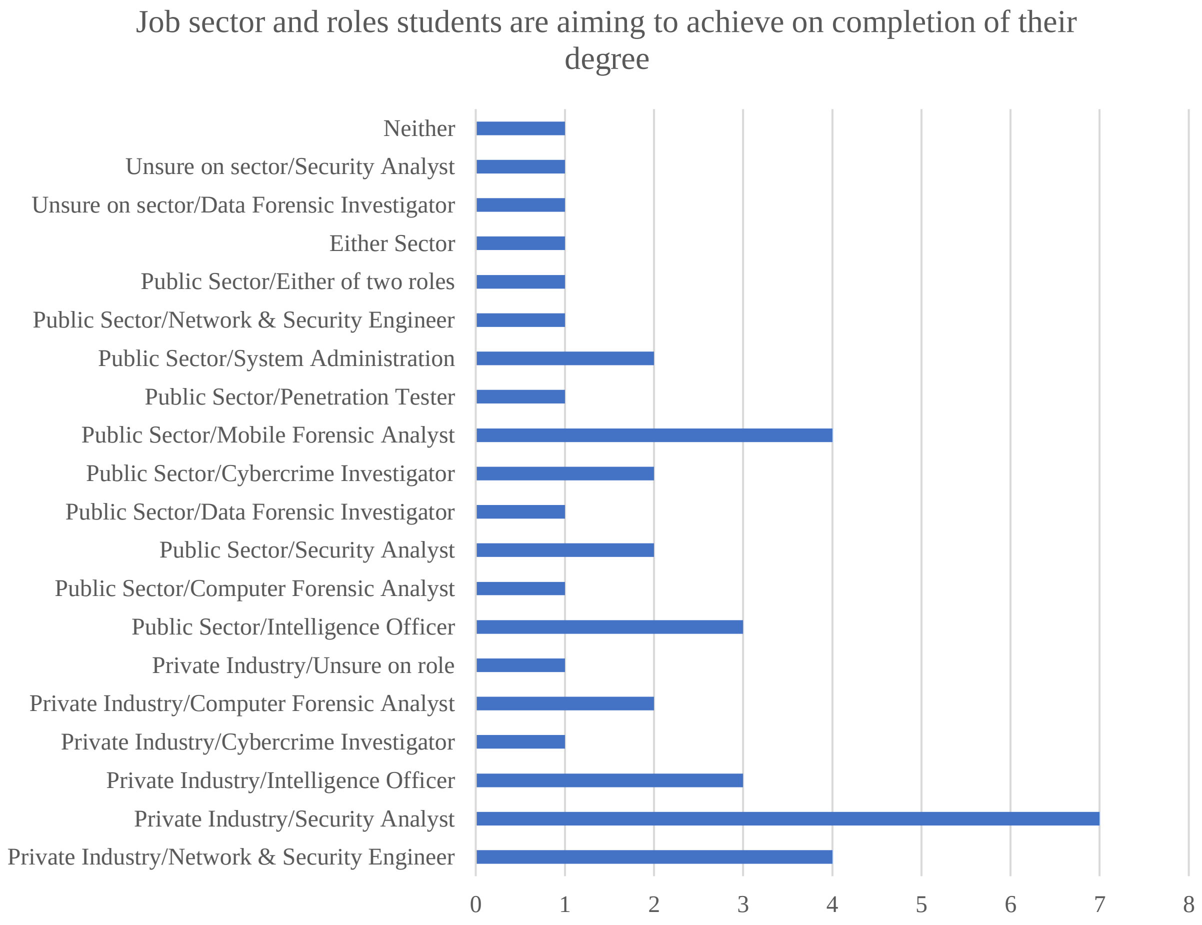


Figure 6.3 – Students' Aspirations for Careers in Digital Forensics/Cyber Security

Across both universities, the most popular specialisms which could be categorised under cyber security were security architectures, malware, hacking and penetration testing and the most popular topic which could be coded as relating more to digital forensics was mobile forensics (Table 6.3).

Students were asked, within the workshop, why they took a keen interest towards cyber security as oppose to digital forensics; for some it was the excitement of hacking and testing systems, while for others it was driven by career prospects and monetary value. Although, it should be recognised that there were still several students seeking a career within digital forensics where students noted there are cross overs with each subject providing them with multiple options when pursuing a career upon graduation.

[31] 'Neither' indicated in Figure 6.3 is a result of one student pursuing the degree for reasons of interest rather than employment.

	University A	University B	
	Total n	Total n	Total n
Specialism			
Security Architectures	8	9	17
Malware	8	7	15
Hacking	7	7	14
Mobile Forensics	1	13	14
Networking	6	8	14
Penetration Testing	7	5	12
Cryptography	2	8	10
Legislation/Law/Policing	4	5	9
Incident Response	5	4	9
Smart Device Forensics	2	6	8
Windows Forensics	4	2	6
Technical Validation Hardware/Software	2	3	5
Linux Forensics	2	2	4
Mac Forensics	1	2	3
Unsure	0	1	1

Table 6.3 – Students' Specialism to Master or View as Most Important in Current Industry

On average students felt they could be earning somewhere between £20,000 and £40,000; breakdown by sector of employment the students identified when pursuing a career can be seen in Figure 6.4. Interestingly, there was overall one less student, aspiring for a career in the public sector in comparison to private industry. However, in terms of wages, the proportion of students who felt they would start on a greater wage was higher in those having chosen public sector as their choice of career progression. This is somewhat different from research by The Office for National Statistics (2017) which shows typically job roles in the private industry pay more.

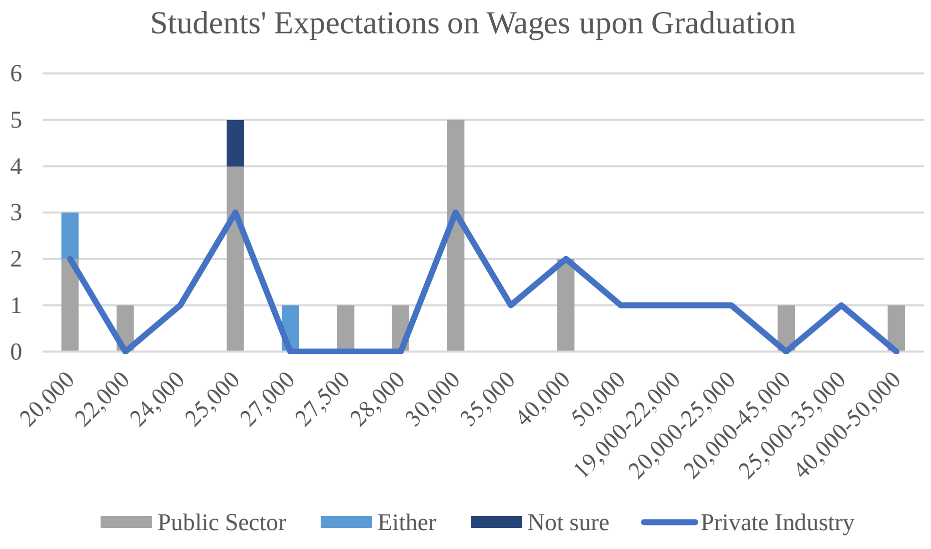


Figure 6.4 – Students' Expectations on Wages upon Graduation

The value of a course after graduating was very diverse among respondents; albeit the consensus that their degree was a steppingstone to their careers. Graduates acknowledged that their progression from assistants to analysts took much shorter time than colleagues with a degree in computing[32]. One graduate expressed their degree:

> "adds a lot of weight to my statements. I can say that I have been university educated in this field. A lot of my colleagues have come in on experience and they have had to show other ways of how they know it all. They are more than capable of doing the job but to a jury they look at it like you are in IT that's not quite the same. Realistically it is but having that piece of paper is useful."

Graduates working in industry, for some as long as three years[33], training and experience in the role have counterbalanced the worthiness of their degree; however, each noted there are still lectures, notes and handouts that they turn to today and found predominantly useful when first starting their roles within the industry. One alumnus recognises though they may not return to their course notes, or where they have become out-dated due to their own experiences, the underlying knowledge they have was learned on the course and ingrained in the work they accomplish. Each interviewee notes that being a digital forensic practitioner means fostering intellectual excitement and knowledge transfer on-the-job where each identify the need for active research due to continuously changing technologies. So, while graduates were able to see the value and weight of their degree on-the-job, this is not necessarily the case when studying.

6.4 Issues with Awareness and Contextualisation

A common theme found among responses from academics and graduates were issues with a student's inability to contextualise information and their lack of awareness for what is necessary or useful throughout their degree. Supporting evidence has been identified in section 6.3.1 remarking on the understanding why certain subjects are taught and how they are delivered on a course. For example:

- some students identified they do not believe their course covers relevant content or is too computing focused;
- some graduates identified they felt their first year of study was too simplistic; while,
- academics identified the need to manage and balance a range of stakeholder expectations and argue that students need to understand the fundamentals of computing[34] to be able to master digital forensics.

[32] Graduate quote: "assistants tend to be experienced, or have a degree, in computing – so they know their stuff but not forensics" so it takes them much longer to move into forensics, some having heard of it taking people several years.

[33] At the time of writing.

[34] A necessary requirement as technology continuously changes yet the fundamentals of computing stay the same.

Furthermore, an academic vocalised: when students leave it is often not the technical or theoretical content which they see are an issue, nor is it necessarily problem-solving skills. The academic believes the challenges are in fact "more the contextual awareness". From the researcher's own academic experience, some students often fail to realise the broader application of the knowledge they are obtaining, the skills they bear where this may spread to the creativity and problem-solving nature required within the discipline. For example, a student's awareness why they are learning about Databases[35] or the importance of Project Management[36] and their purpose on a digital forensics course, within the discipline and how they relate to industry skillsets. Arguably, this may relate back to the need for academics to clearly manage expectations and be direct as to why and how topics, skills and approaches to learning relate to professional knowledge and skills required. One academic epitomises this recollecting their own degree experience[37], discussing how it took a long time before they, themselves, realised the skills they were learning on their degree were those which were accepted in order to do specific jobs. They admitted how "no one spoke about it very much … and said you need to understand those concepts. It's not that you are going to sit down day in and day out and do this, but you do need to understand it."

The researcher argues that this is likely still the case with many degree programmes and was epitomised by one graduate who discussed with the researcher how they felt they were misguided at university when it came to the importance of forensic principles and procedures. Digital forensics in the UK is enriched with guidelines and standards which are considered the main reference for practitioners (analysts and responders) towards keeping data unchanged and ensuring laboratory compliance (e.g., ACPO Good Practice Guidelines (ACPO, 2012) and ISO 17025 (International Organization for Standardization (ISO), 2017)). While areas of cyber/information security also adhere to a code of practice (e.g. the Information Security Standards ISO 27000 Series (International Organization for Standardization (ISO), 2018)). Literature reviews and examination of numerous phases of a digital forensic investigation have been seen over the years yet, the discipline cannot account for a definitive nor extensive methodology. The graduate recognised an attitude where they "thought eh" when they were a student. It was not until they were in the job that they realised "no, I do need to stick to these." When asked why they felt they had been misguided they described

> "I think it is one of those things you just think eh. It is just one of those things that your lecturer tells you. However, there is no strict guidance for us, and it is the only thing there

[35] Of the 39 students in this study, only 53.8 percent (cumulative) rated the topic as being Very Important or Important to such a degree (see Appendix D – D.2.1).

[36] Of the 39 students in this study, 6 felt project management was Not Important at all, while 3 felt it only Slightly important and 7 moderately important (59% of students felt it to be of higher importance).

[37] Degree obtained in a different subject.

> that we have to back us up. For example, if we are in court and are asked why we turned the device on, we can say because the officer said it was fine. There is a lot of stuff that can go wrong here. I think the audit stuff for students is good; to get used to logging everything you do."

Discussions with one academic also pin-pointed the intrinsic importance of these processes and principles in digital forensics and how they can often lead students to question the methodology and outdatedness of these. For instance, the interviewee notes;

> "The students start thinking for instance that there must be steps [to] go through, there must be a methodology as to how to forensically analyse ... I [the academic] have to say no, there is not as every case is different. The students find that very difficult to get their head around. They have huge problems with the fact that there is not a methodology to follow, so sometimes that defeats them or inspires them to go off and do something else."

A simple example of a lack of methodology within the subject is mobile technologies where the acquisition of data from the device can be more technical and invasive than the traditional hard drive where you would make an image (a bit-for-bit copy) to work from. There are five levels of acquisition in mobile forensics and some involve more electronic engineering, e.g., Chip Off forensics, where there is a higher risk of destruction or alteration of the chip itself. The process requires the physical removal of the memory from the device to extract data and in turn alternate levels of forensics may not be possible. In line with the ACPO Good Practice Guidelines (ACPO, 2012) practitioners are meant to avoid taking any action that can result in the alteration of data which may be relied upon in court unless the analyst is authorised and technically competent to do so. Within those boundaries the practitioner must also provide an audit trail and record all processes and evidence, so the same results can be obtained by a third party. In the case of Chip Off forensics where the destruction of the chip during extraction is plausible, it is not always then feasible to adhere to principle one: no alteration, or principle three: replicability of the investigation (ACPO, 2012). Though the documentation outlines that these intrusive and destructive methods may be subject to this level of investigation when necessary and in accordance with the "examination levels … outline in the NPIA mobile phone SOPs" (ACPO, 2012, p. 11), this presents that there is not always a methodology to abide by which suits the current technologies and principles.

Academics interviewed believe "students are [often] attracted to the course because of the practical and interesting material"[38]; however, students then realise there is content which is less appealing or less

[38] Supported by student expectations and initial views, discussed above.

practical and this does not meet their expectations. Academics recognise students "need to have some of these things … [however, some are] very difficult to experience". Examples include students "realis[ing] there are policies and governance and that it is not as interesting" where guest speakers are often called upon to talk about such topics. Academics discussed how they try to ensure students realise the potential of the topics covered on their courses, knowledge and skills gained and more, however, they felt it was often of increased value when vocalised by an external guest such as, an industry professional. Many universities arrange for credible 'experts', or alumni to give insightful and skilful masterclasses to students where guest speakers can often enhance the material covered on a course and provide students with relatable scenarios and a sense of career prospect. This is something which has long been exercised at CCCU where industry professionals as well as previous graduates are welcomed to give masterclasses, speaking of their careers and degree experiences. The researcher has observed students benefiting from, in particular, graduate guest speakers via this approach as the two stakeholders can relate with one another: graduates reflecting on what they learned and how they got to their current role providing insight for the students and, the students relate to degree experiences and the search for employment. Furthermore, student workshops in this study provided similar experiences where the researcher, as the guest, could identify these issues and benefits while acknowledging other academic views of the workshop being able to "provide[] students with an element of critical thinking", often reiterating aspects which their own academics have tried to address and voice.

One academic does recall how a speaker is not always "the best mechanism … [however,] it is better than not tackling [subjects] all." Guest speakers can provide win-win situations for all stakeholders, an engaging solution to less interesting topics and a bridge between the gap of theory and practice. However, they can lead to issues where students are unable to contextualise the content they have learned with the presenter's experience. The researcher's role in academia has witnessed students often unable to respond to guest speaker questions, unexpected sets of blank faces and the need for speakers to cover issues in more basic depth than necessary. Approaching the students, the researcher often found that students were unsure, vague or afraid of responding to questions "in case they get it wrong". Similar findings were discussed by an academic who provided an example where their guest speaker spent ten minutes or so trying to explain the difficulties around changing a password policy because "it was quite obvious that [the] students could not grasp how this could be such a difficult thing to achieve and [how they] think that is one of the weaknesses of graduates coming out of university in a security area."[39]

[39] Similar discussions were had with professionals who had taken time to give guest lectures at universities (discussed in chap.7).

To compare, graduates interviewed within this research were asked several questions which asked them to think back to their student days, each graduate recognised they were not always able to appreciate the applicability of course content to the role in industry. One graduate epitomised this stating how the parts they learned that were most useful "were none of the parts [they] thought would come in handy." Other discussion points included issues with understanding why some subjects were being taught in vast theoretical depth; after all, it is a practical discipline so this questioning could be argued as a valid reservation (further discussed in section 6.7).

Furthermore, three graduates interviewed from the same cohort of students discussed with the researcher how people on their course complained about the course to their peers; describing the course "to be a waste of time". This was something the researcher, as an academic, noted of the cohort at the time. Selected individuals openly expressed they did not feel as if they had learned anything and "nothing they had learned would apply in the real-world". The three individuals spoke of how they disagreed with the negative peer comments about the Forensic Computing programme, one stating they felt these students were wrong:

> "[the course] was teaching you the basics of file systems without you knowing it like doing the file carving and just the basic concepts. Let's be honest doing a degree in forensics is too short a period to learn and know everything. No matter what modules you are taught, you are still going to start knowing nothing … and just be even more ignorant about slightly different things. Hopefully it gives you the basic principles rather than the exact knowledge. You don't need to know, for example, where a registry key is for something, but you do need to know well, here is the Windows registry. You do not need to know how every file system works, but you do need to know this is what journaling is, this is how file tables work … just the general concepts. You don't need to know how many offsets a piece of data is into the Hex because nobody knows that for real, you just have your own notes that you refer to for those things."

Furthermore, acknowledging that the people who complained have not ended up in good jobs and that "if you do the basics [of a course] you will pass, then that's about it. If you do what you need to do outside university as well then you learn a lot more." This was a key theme among graduates. Particularly, being "encourage[ed] to look elsewhere and do some more research on topics" recognising that while "it would be nice to be spoon-fed this stuff, you don't have enough time." Reiterating how the course gave them

> "a decent grounding to start here [in their current role]. There has been nothing that I have been completely out of my depth on. I have always covered part of it to know

> what's going on and to do a little more research myself. I think the best thing about it was the breadth of knowledge, especially the tests we had initially to get this job. It was around 150 questions covering everything from converting number systems and everything in between … You can't be an expert on everything."

The lack of awareness and contextualisation is something which professional responses in chapter 7 also address, referring to disadvantages of graduates seen in industry today. Be it the lack of confidence or awareness and applicability of what they have learned, employers are looking for students to demonstrate the specialisms, skills and fundamental knowledge they have learned on their degree; something which is not always achieved.

Another notable example of the lack of awareness and benefits of real-world application of theory-practice links to ensuring a valued degree experience included a graduate who recalled the heavily theoretical learning applied to Cryptography, and how it was not until they were called to court where they had to explain, in layman's terms[40], how encryption worked that they saw the benefits[41]. While the graduate felt there was little practical work, they identified that the assignments provided problems and scenarios which were realistic. However, the graduates continued to note that there was still a little too much theoretical detail in Cryptography lectures and lab classes. The graduate also discussed how there was content they "didn't think would be useful like calculating the size of your disk and how many sectors are missing" noting these as important aspects required in statements. They continue to note that "statement writing might be useful at the end of second year to put it all in place of why, especially when you have to explain to someone else who does not have a clue", reflecting on contextualisation of content on the course.

In most recent years, court room training[42] has been introduced at CCCU for students to provide them with experience of court room scenarios, witness statements, report writing and note taking measures, aspects which graduates felt could be improved on the course. Graduates communicated they received this in part but felt that it was not content which "was really focused on; it was more the technical side of actually how to do it". Expressing, for example, skills required for statement writing where they were left feeling there needed to be more on "what it is, and then how to explain to a layman and to a jury the technical details". Although, a necessary improvement this had been taught very quickly on-the-job. This suggests that awareness needs to be addressed by academics and while learning and teaching methods employed provide insightful knowledge growth, applicability can be the biggest issue and add affect to unrealistic career

[40] To explain complex and technical jargon using terms and words that any individual can understand e.g., in this scenario for the jury.

[41] However, many of the graduates continued to note that maybe there was still a little too much detail in Cryptography.

[42] Bond Solon Training

expectations. Alumnus were able to recognise that academics had made effort to manage issues of awareness by promoting students to attend cases at local courtrooms to witness what happens, however, some graduates reflected that it's worth "wasn't necessarily appreciated". It was suggested instead that a full investigation in the form of a larger scenario-based learning exercise would have been ideal at the beginning of the third, or end of the second year. Reiterating that this would have been useful to conduct again at the end of the third year as it would allow students to recognise and draw upon all that they have learned. The feeling that it would have been useful to experience an investigation from beginning to end including aspects of collection, analysis, continuity, recording, report writing, witness statements and so on (i.e., a range of investigative skills and abilities) was a prominent theme[43].

The researchers own active teaching experiences show that students do not always recognise the applicability elements of theory and practice nor suggestions until on-the-job application. For example, an alumnus who gained industry employment emailed the researcher to obtain a copy of a script they had been asked to devise using Bash in a third-year assessment, which they had not kept hold of. The individual had been asked to perform a work task which had been covered by the assessment; specification included below. While another graduate recalled how they "forgot to download [their scripts] and lost them" stating "it would have been so useful, however, I was fortunate that they [their workplace] had some already in place". The scenario-driven approach of assessments shows how assessments within a degree programme attempt to include realistic tasks and while the graduate was unable to recognise this at the time, they were able to apply in context within the workforce. Arguably, this supports the growing need for collaboration with all stakeholders within digital forensics to provide more scenario, reflective and practical learning along with external discussions/management of expectations and management which aid student's awareness and contextualisation of pertinent learning for employability.

Assessment Specification

The script would search through directories and sub-directories creating SHA1 hash values for each image found, using these values to compare and determine whether any duplicate image files were present. Students were then tasked with reporting and representing relevant information of their choice about the dataset, including a count of duplicate items. Information would include, hash values, filenames, file paths and other file details. The script would be used to make a copy of each unique image to a new output directory for further investigation. Students were asked to include testing documentation, any justifications, assumptions, explanations, and limitations of their script.

[43] This is something now being explored at CCCU to provide a longer and wider investigation encompassing all-in-one.

6.5 Subjects and Skillsets

Newly devised frameworks within cyber security and digital forensics have shown highly important topics across the discipline, particularly focussing on the fundamentals of computing, computer forensics (e.g., OSes, networks, legislation/ethics, investigative techniques and analysis and practices). This was somewhat supported by analysis of courses in chapter 2 where review showed each of these key topics. Similarly, one academic with over 20 years' experience highlighted how their course aims to provide basic building blocks in computing and forensics at level 4 including topics such as, computer systems and programming. While level 5 looked at more technical and practical aspects such as, investigative analysis of file systems, tools and techniques, software creation, professional and ethical responsibilities, and integrity. Level 6 developing students for employment looking at, for example, case management, professionalism, expert witness, and integral notes.

Course documentation often supports these outlines and identifies the development of technical and vocational skills which are expected of a student upon completion of a course, examples include:

- understanding of the scope, concepts, principles and theoretical underpinnings of computer forensics and security.
- awareness of legal, professional and ethical considerations in the field of computing and forensics/security.
- an understanding of the characteristics and operation of various networking technologies and operating systems.
- use of a range of programming and database skills to assist in forensics and security investigations.
- use of a range of software tools for application within computer forensics and security.
- use of forensic investigation tools and other techniques to gather evidence in a forensically sound manner applying appropriate theories, concepts, and principles.

While previous sections in this research have pinpointed how responses can identify issues with awareness and contextualisation, this study looks further at capturing ideal subjects and skillsets expected of a professional in digital forensics in order to reflect on industry expectations, course provisions and student perceptions. To do this, graduates were asked to reflect what topics they felt had been useful and applicable on-the-job, while academics were asked to discuss topics they felt industry partners felt were shortfalls within the discipline and education. In addition, first-year students in this study were asked to identify the subjects they felt were important of a digital forensics and/or cyber security course.

> "I think all of the modules support each other in a way. I don't think I could look back and say I could definitely have missed that module and got the same experience at the end of the day." – Graduate Participant

Undoubtedly, each stakeholders' views, ideals and opinions would be subjective and reliant of their own experiences within the discipline[44]. A setting and curricula which invokes "intellectual excitement and discovery" for students to realise the value of what they are learning is important (Ahmad and Maynard, 2014, p. 516). This study considers part of this to be the awareness and contextualisation of content, subjects and skills for study and industry progression. Among the stakeholders of this study[45], key topics were identified to be important for a digital forensics course from graduate recommendations, student ratings and academic discussions inclusive of views of skills-shortages and industry expectations.

This section continues to look at these topics in further detail where topics included:

- fundamentals of computing;
- basic forensic principles and procedures;
- programming and scripting;
- databases and networking;
- Windows, Linux[46] and Mac forensics;
- mobile device forensics;
- network forensic investigation;
- cloud forensics; and,
- live data forensics.

6.5.1 Fundamentals of Computing and Basics of Forensics

> "It is the nuts and bolts of file systems … there should definitely be a module on file systems on courses". – Academic Interviewee

Graduates interviewed felt that current students/graduates looking to pursue a career in digital forensics must possess foremost the foundational skills and knowledge of computing and forensics to be able to successfully acquire a job and progress in their career. All graduates stated knowing the core skills is probably the best bit. One graduate noted how the "principles should be burnt into them [students] and that is pretty much what you need to know; it is mentioned here [in their employment] a lot". While previously,

[44] As comparison professionals were asked to identify topics and skills they would expect, discussed in chapter 7.
[45] Academics, Students and Graduates.
[46] Including as an investigative tool.

this study has highlighted how graduates as students have not been able to recognise their importance meanwhile academics try to promote their intrinsic importance. Graduates also acknowledged that an important and demonstrable skill within a digital forensic practitioners' role is the requirement and ability to document their workings, findings, authorisations and more using meticulous notes and often photos. They stress how important making accurate, precise and informative notes are to providing an audit trail (ACPO principles) and for their own purposes; a basic forensic procedural skillset.

Furthermore, it is interesting to note that graduates distinguished that the knowledge they had gained and skills in knowing how to manually file carve, understand signatures and essentially what the tools are doing not just how to use the tool is paramount. This was supported by academics who were able to highlight how, what can be described as, "lower-level tools" and open source tools can be used to show students how, for instance, files are stored and hidden as well as carved out of a file system. While academics noted how they use "higher-level tools" (e.g., those of proprietary nature) in the curriculum, this is often so the students gain awareness of, and are familiar with, the tools and apparatuses they will be using during their employment in industry. Many noted that these tools can be learned far better through the initial use of low-level tools with additional training courses, for which there are many, provided by tool providers on completion of their degree on-the-job. One academic articulated:

> "the first thing I would hope they do not encounter at all is the push-button forensic tools … because it is a button you push you are isolated from what is happening. … to be an expert you need to be able to explain what is going on. So, in law enforcement you have to be able to stand up in front of a judge and jury and you have to be able to persuade them why you should be there and that you really know what you are talking about and also that the evidence that you have found is correct. … pushing a button and a piece of evidence appearing does not allow an individual to understand where the evidence was found or other scenarios such as, why it could not be seen through a Windows file explorer, for example. … [That sense of detachment from the forensic process,] "isolation by higher-level tools" … Lower-level tools should be used to show how files are [stored and carved out of a file system] … individuals would do much better in training courses for tools having learned [through the lower-level tools and having gained an understanding of file systems]."

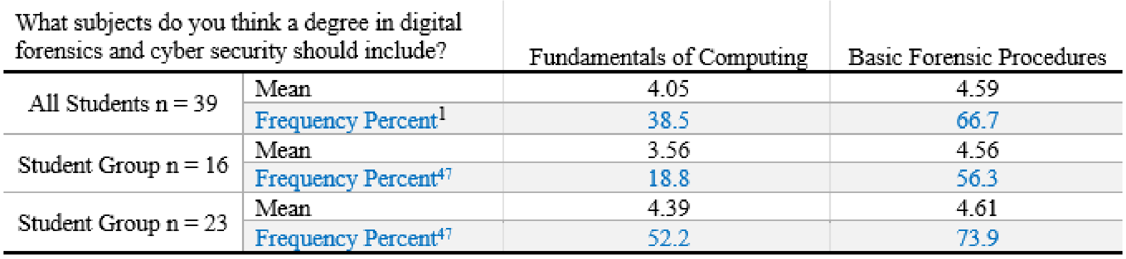
Furthermore, academics discussed how important general computing fundamentals such as networking and databases were paramount to a digital forensic investigators ability to conduct forensic and security investigations. Additionally, how procedural and principles of forensics were something which academics noted to be fundamental to a student's learning, though curricula at institutions had often changed to support digital forensics and cyber security beyond policing in wider remits including corporate environments.

Essentially academics discussed how there needed to be a baseline of computing knowledge to understand how to forensically analyse digital devices or protect systems. One example and disadvantage one academic mentioned looked at the inability to interpret data manually epitomising this stating:

> "consider the key skill at introductory level to be the ability to manually interpret hexdumps. If a student cannot do that, then there is no point in them continuing because at some stage, and how I justify it is, that there is not always a tool to do what you want to do. We are in an area that moves that we cannot keep up with. You encounter new things fairly regularly; there is no Google Search that helps, there is nothing like this. So, new file systems … they don't come out that often, but they do cause hassle when a new one appears. [Take] communication apps on your phone there seems to be a [multitude of] new ones each year … there is not necessarily a forensic tool to analyse them. That example, you have an advantage as a lot of them are SQLite based nowadays so again you go back to first principles, teach general SQL rather than teaching analysis of the Firefox Browser … so they can actually analyse an unknown database themselves. So, I think really it is some computing fundamentals that are the key skills where they can then apply them themselves and apply them in new situations."

While graduates identify that their roles often rely on the standard industry tools, they acknowledge that having the knowledge and skills to be able to manually carve out data or understand Hexadecimal offsets is key to their baseline knowledge.

Students meanwhile felt both topics, fundamentals of computing and basic forensic procedures are important for a digital forensic course. Though descriptive and frequency statistics show the students from both groups felt the basic forensics procedures to be more important than the fundamentals of computing as shown in Table 6.4 below.



What subjects do you think a degree in digital forensics and cyber security should include?		Fundamentals of Computing	Basic Forensic Procedures
All Students n = 39	Mean	4.05	4.59
	Frequency Percent[1]	38.5	66.7
Student Group n = 16	Mean	3.56	4.56
	Frequency Percent[47]	18.8	56.3
Student Group n = 23	Mean	4.39	4.61
	Frequency Percent[47]	52.2	73.9

Table 6.4 – Student thoughts on Computing Fundamentals and Basic Forensic Procedures

Further statistical analysis of student responses conducted using Principal Component Analysis (PCA)[47]. Seven components were extracted during this analysis, eigenvalues were then plotted, and a curve of distribution identified where "only the factors to the left of the point of inflexion" are kept, this is where the curve drops (Field, 2013, pp. 677–678). This was approximately a 30-degree angle as shown in Appendix D – D.3 (p.367). The strongest components were extracted and considered, for they account for the greatest proportion of variance, where they were rotated (Rotated Component Matrix) to equalise the variance among the components. The curvature showed that both components 1 and 2 should be considered. These were named *Digital Forensics Fundamentals* and *Computing Essentials* based on the grouped topics. Results from further analysis showed student responses for the first component: 'Digital Forensics Fundamentals' included highly correlated ranked topics such as live data forensics, mobile forensics and digital forensics tools (proprietary) as seen in Table 6.5, demonstrating a strong relationship. While 92.3 percent of all students felt that basic forensic procedures were either Very Important or Important, what was interesting to see is how Basic Forensic Procedures did not correlate with the topics grouped under digital forensics fundamentals (Appendix D – D.2.1).

		Cumulative Percentage (%)			
Topics	Rotated Component Matrix Value	Very Important/ Important (>75%)	Very Important (>50%)	Means Statistic	Number of Students (n) [48]
Component 1 – Digital Forensics Fundamentals					
Live Data Forensics	0.865	89.5	50.0	4.39	38
Mobile Forensics	0.836	86.8	60.5	4.45	38
Digital Forensics Tools (Proprietary)	0.822	86.6	68.4	4.50	38
Digital Forensics Tools (Open Source)	0.749	89.5	63.2	4.53	38
Linux Forensics	0.744	81.6	47.4	4.26	38
Linux as an Investigative Tool	0.724	78.9	36.8	4.16	38
Mac Forensics	0.684	73.7	36.8	4.05	38

Table 6.5 – Rotated Component Matrix (PCA) for Component One (Digital Forensics Fundamentals)

Component two: 'Computing Essentials' presented a pattern among topics which include: Project Management, Computational Mathematics, Software Engineering/Development, Fundamentals of Computing and the Internet of Things (Table 6.6) showing that the second component suggests it is most highly correlated with Project Management and Computational Mathematics (Appendix D – D.2.1). This topic included 'Fundamentals of Computing' where 15 students felt the topic to be Very Important and another 15 classed this as Important when ranking given topics; a total of 30 students (76.9 percent).

[47] See Appendix D for detailed statistical analysis.
[48] One student did not rate these topics.

		Cumulative Percentage (%)			
Topics	Rotated Component Matrix Value	Very Important/ Important (>75%)	Very Important (>50%)	Means Statistic	Number of Students (n)
Component 2 – Computing Essentials					
Project Management	0.827	59.0	28.2	3.49	39
Computational Mathematics	0.758	44.7	15.8	3.37	38
Software Engineering/Development	0.626	33.3	12.8	3.15	39
Fundamentals of Computing	0.621	76.9	38.5	4.05	39
Internet of Things	0.589	66.7	35.9	4.00	39

Table 6.6 – Rotated Component Matrix (PCA) for Component Two (Computing Essentials)

Referring to descriptive statistics for these topics yield findings which highlight students showed little interest towards the level of importance of topics such as, Software Engineering/Development and Computational Mathematics. Cumulative percentage of both 'Very Important' and 'Important' responses accounted for only 33.3% and 44.7% respectively. In comparison the Fundamentals of Computing was noted in the table in Appendix D of relatively high importance with a cumulative percentage of 76.9%. This component yields a mix of topics deemed, by the students, as least important yet shows common variance among their rated responses.

6.5.2 Programming

Across the discipline the debate over the inclusion of programming in a forensics degree and to what degree has always been an issue among students and employers. From the researcher's own action research at CCCU, they have found that it is rare that students looking to take, or studying, a course in digital forensics are keen programmers. From experiences working open and applicant day events, teaching introductory programming and programming in relation to forensic and security tasks, individuals often express their dislike towards the topic. A common question asked at open days for the computer forensics and security course by potential students include "how much programming will there be on the course?". Prominence is of some concern for the applicant and their experience or ability to program.

Similarly, in a digital forensic and ethical hacking class held in 2018, the researcher asked a group of 18 third year students their interests in programming and the career they wished to pursue. The class identified careers in cyber security and expressed little interest or enjoyment for programming, many contemplating their dislike toward such activity. This is a similar result to year one students discussed below.

The researcher was able to use some discussion time to highlight the importance of programming in roles particularly related to cyber security. At this point it should be noted that the last time this third-year cohort of students conducted an element of programming was in their first year for C#. Since then the students have received an extensive scripting experience using Bash for Linux forensics and as an investigative tool, while also focusing on Windows forensics using well-known tools and manually. Yet, their ability to contextualise the importance and necessity for programming in a career they wish to peruse is again something which can be highlighted

Considering these 39 students' responses further, they were questioned and provided with the topics 'Scripting/Programming' and 'Software Engineering/Development' and were asked to rate their perceived importance on a digital forensics and/or cyber security course. The mean value for each of these fell below 4.00[49] with a majority of students rating these moderately important, as shown in

Figure 6.5. While programming for these students was not highly rated, it can be inferred that some students are able to recognise the importance such knowledge/skillset can have for a practitioner in cyber security and digital forensics. Table 6.7 highlights the difference in ratings for both items, where one can see the mean at University A was substantially less than that of results from University B, particularly for 'Software Engineering/Development'.

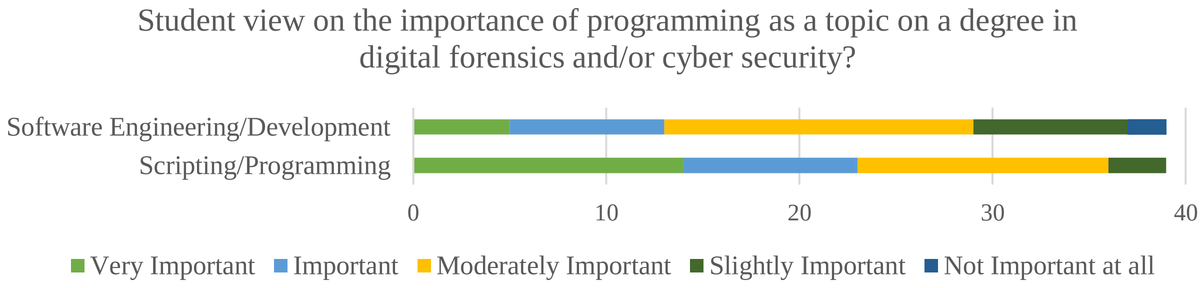


Figure 6.5 – Student responses: importance of programming on a digital forensics and/or cyber security degree

What subjects do you think a degree in digital forensics and cyber security should include?	All Students n = 39	Mean	University A Students n = 16	Mean	University B Students n = 23	Mean
Scripting/Programming	39	3.87	16	3.81	23	3.91
Software Engineering/ Development	39	3.15	16	2.88	23	3.35

Table 6.7 – Student thoughts on Programming on a Digital Forensics/Cyber Security Degree

This coincides with graduate views expressed in interviews held with the researcher. Discussions included the need for university courses to ensure that they "update the languages courses are using" particularly as

[49] 4.00 was the mean value cut-off used for statistical analysis. However, the mean value for Software Engineering/Development: 3.15 and Scripting/Programming: 3.87 showed a moderate level of importance (an average mean of 3.51).

schools are coding as standard. Chapter 2 noted how all universities within the UK include an element of programming on a course in digital forensics and/or cyber security. However, graduates held a range of views on programming during their intake at CCCU. These ranged from the course being ideal as it was less programming-oriented[50] to others who felt the modules, particularly in the first year, to be "too simplistic"[51].

Alumni responses included discussions such as:

- the course was less programming oriented (unlike Computing or Software Engineering offerings) and this swayed them to pursue a course which was not aligned to becoming a professional computer programmer, particularly where they felt it was not their strongest skillset[52],
- for some graduates, the basic programming at level 4 was too simple and they observed two groups within the lab classes, "the group who knew nothing and the group who felt 'this is super old hat and I'm bored' [where they expressed] there seemed to be nobody where it was really interesting";
- programming modules at levels 5 and 6 juxtaposed with this and were more stimulating and advanced including take home questions requiring more problem-solving and research;
- level 5 operating systems included too much programming and graduates felt there was a need to focus more on aspects such as the Kernel and building Operating Systems.

Discussions with academics identified that programming is essential on courses and within the industry. This was supported by alumni who agreed on the importance programming plays in their practitioner role. Acknowledging that one "do[es] not need to be a software engineer, but [one] do[es] need to be comfortable whipping up something small and simple". Something which alumni in this study had often resulted to on occasions where simple, or extensions of, tools were required. Recognising that you have to be comfortable with the fundamental knowledge of how to program, how programming languages work and when these skills are useful and applicable. Academics also recognised that level 4 study modules are used to ensure all students have a baseline of knowledge before continuing with more advanced learning[53].

[50] The researcher has experienced this at Open Days and Applicant Days for potential students who often want to avoid or refrain from doing too much programming. Here an applicant's expectations have to be managed to reiterate the course includes programming and how it is an important aspect in the career of a practitioner.

[51] In the previous revision of the course programming and scripting languages included Visual Basic, HTML, Bash and the C language. In the reviewed course these have been replaced with C#, Bash and Python to reflect industry and address graduate observations.

[52] This has also been a continued observation on behalf of the researcher in an academic role with students and applicants to the former Forensic Computing Degree, now Computer Forensics and Security Degree.

[53] Taking into account differing backgrounds/levels of previous education prior to attending university.

Further analysis looking at graduate responses for issues with the first year of study being too simple saw other topics mentioned. One graduate expressed "the first year seemed at a lower level than [they] had anticipated, apart from the digital forensics modules … which was the only part of the year which [they] found particularly challenging and the most interesting." Another noted that "by the time you got to the second year you really got into the nitty gritty bit of it." These responses link, once again, to the management of expectations on behalf of an academic and the need to ensure students feel like they are achieving learning and engaging with the course across all years of study.

These responses may raise questions such as is it necessary to have a first year in a Bachelor's degree if students feel some topics are too simple or unrelated, and it's worth when it does not count towards a student's final grade. There are several considerations which must be made, for example, the contextualisation and applicability judgement of the student as well as the varying background, skills and attributes a student may possess. Conceptually students seem to have mixed views of which is harder, A-Levels or the first year of university across degree programmes as seen on known student forums (The Student Room, 2000) and in the researcher's experience as an academic.

6.5.3 Databases and Networks

Databases and Networks are just two topics which are prolific for an investigator. For example, mobile applications and their use of databases to store, for example, social/messaging content, contacts and more as well as the availability, transmission and logging of network connections and traffic. These are even more prevalent with the invention and application of Smart and IoT devices where Conti *et al.* (2018) highlight how "[t]he Internet of everything is developing a haystack which contains lots of valuable forensic artefacts" and how the scientific process/investigative phases such as, collection, preservation and analysis see forensic challenges notably due to network and cloud based workings.

With this in mind, students of this study were asked to consider the importance of both topics for a course in digital forensics and/or a cyber security. Results show that both sets of students perceived networks to be slightly more important (Table 6.8). Where 53.8% of students rated Networks as Very Important comparable with just 28.2% for Databases and 38.5% of students expressed, they felt Databases were only 'Moderately Important'. This is an intriguing result considering database knowledge is critical for analysis in both digital forensics and cyber security where, for example, social applications use database files (.db) to store data on mobile devices and may be useful in a forensic investigation, and cyber-attacks include examples such as, SQL Injection attacks which use SQL databases to gain unauthorised access to sensitive data.

What subjects do you think a degree in digital forensics and cyber security should include?	All Students n = 39	Mean	University A Students n = 16	Mean	University B Students n = 23	Mean
Databases	39	3.74	16	3.88	23	3.65
Networks	39	4.33	16	4.25	23	4.39

Table 6.8 – Student thoughts on Database and Networks on a Digital Forensics/Cyber Security Degree

This is also interesting as course analysis (chapter 2) demonstrated that networks and database are two essential pillars of learning on a digital forensics course. Keyword search found 'Network' mentioned on 74 occasions and 'Database' on 32 occasions. However, forensically both network forensics and database forensics were mentioned on fewer occasions.

While these student perceptions may demonstrate the feeling of topics such as, basics of digital forensics and ethical hacking and countermeasures to be more important, it may also imply a lack of awareness and contextualisation for the underlying worth of specific topics. This is supported by graduate responses which demonstrated reflection to their time studying as a student and their inability at the time to recognise why databases and networks were so important to their learning. One graduate stating: "I think Databases … when I did it, I thought why am I here?". However, reflecting on their industry experience and, on application in a role in corporate forensics, the interviewee explained they could instantly recognise the importance of the subject due to the company "us[ing] a lot of SQL". They identified that out of a team of 50 people they were the only one with experience of SQL at university; all other members of staff were self-taught. The graduate felt they then "had a massive advantage" continuing to acknowledge that in their current role they also use SQL professionally, reflecting how they "wish [they] had carried it on to the next year". Database knowledge has previously been noted as one of "the five pillars of an IT Curriculum" for several years (Rowe, Lunt and Ekstrom, 2011, p. 115).

Meanwhile, other discussions with graduates focused on the depth of theoretical learning on network-based modules at CCCU. Participants views toward networks were disparate with some noting how specifically networking content from the course was less useful in their industry role and how its predominance would have been beneficial for roles such as network security analysts. One graduate gave the example of "understanding the underlying aspects of TCP and UDP and the way they work". While, another graduate using more networking knowledge in their role felt that the course "went very far in-depth" yet they only use "a higher-level view" of networks not to the "byte level, packets or structure of packets" which were taught on the course. This shows that while alumni do not use all the knowledge they gained important to them are the skills they obtain which translate to the day-in-day out role of a forensic practitioner and a consensus among graduate participants documented the "concept of networks helps a lot with everything" and the fundamentals provided were good yet, learning about networks is very different to how you forensically handle networks; something they would have benefitted from more.

While forensic analysis requires an underlying base knowledge of networking concepts, graduates felt their course curricula required tweaks to address practical network forensic investigation. This is something loosely indicated by UK course provision analysis in chapter 2 where, fewer modules indicated mobile forensics, Linux, database forensics and network forensics; all areas graduates noted as being useful. This demonstrates that while courses may provide a wealth of networking concept learning there is arguably need for students to acquire practical skills in networking forensics. Graduates pointed out how, for example, you need to know the fundamentals of Mobile IP and TCP/IP, you need to be comfortable looking at PCAP files and you must understand Network Address Translation (NAT). An example at CCCU is the use of Wireshark[54] lab classes, among others, which are used to introduce students to network forensics where representation of network packet data (e.g., PCAP files) allows students to apply theory to practice; for example, theoretical learnings such as, the TCP 3-Way Handshake where network packet data is represented in human readable format typically packet-by-packet and by ISO layer through to extraction of network artefacts from protocols such as HTTP and FTP. Graduates experienced a small number of lab classes[55], and the interviewees who mentioned network forensics left the researcher feeling there needed to be more theory-practice links through application of networking lectures and forensic practicals on the course to enable students to become competent on completion of a digital forensic course to conduct investigations reliant upon networking data. One graduate further linked Linux modules with their understanding of networking in relation to server setup and analysis as well as Operating System modules for their understanding RAIDs. However, the graduate acknowledged the underlying understanding and theory is one thing, forensically handling RAIDs is “a whole different story [and] recreating [them] in EnCase is a massive learning curve” where they would have benefitted from a practical forensic approach to these learning situations.

6.5.4 Windows, Linux, and Mac Forensics

Graduates noted how practitioners are expected to be acquainted with well-known operating systems such as Windows, Mac and Linux and their file systems where recent educational frameworks list multiple OSes and the need file system analysis. Ample knowledge of these different operating and file systems requires, to some extent, experience, and on-going investigation. Where responses often directed back to awareness, contextualisation, and the need for on-the-job practical application for theory-practice links.

[54] https://www.wireshark.org/

[55] At the time of the old course.

Within educational digital forensics, Linux is often used as a tool to help students understand basic concepts (for example: file carving, cryptography, security), as an introduction to Mac forensics and to demonstrate how tools can be developed along with programming/scripting languages to extend open source or proprietary tools to deliver specific tasks yet designed or further to corroborate tool findings (Anderson *et al.*, 2006; Stephens, 2012). Academics supported this concept when interviewed, portraying its usefulness in enabling students to understand and apply the theory associated with how a computer system works, manually being able to carve out data, and provide the ability to question tool outputs while also conducting hands-on investigations when there are no recognised tools to turn to.

Alumnus were also able to recognise these advantages and how the delivery of Linux (OS/investigative tool) was a topic and skillset that has been widely applied within their career and provided them with familiarity and a sense of comfort when working in an environment, an asset to their foundational forensic knowledge. One commenting that,

> "the Linux/Bash stuff was really useful to learn the ideas of carving and hashing and things. However, I have only had three Linux jobs so far in the year I have been here, and I have done 70 jobs. Again, I am only extracting it and looking at it within a tool, so not really using Linux."

While this graduate recognised they are not really using Linux but the familiarity is useful, another graduate highlighted that in a regular digital forensics high-tech crime unit "you may only come across a Linux box once in a blue moon", while in more specialist units they are often encountered "in almost every case [when] dealing with hacking, DDoS attacks, botnets [and so on] … where universally, in [their] experience, [they] are dealing with Linux machines". Furthermore, identifying that "learning Linux as a steppingstone into Mac forensics"; describing Linux as a "sleeper hit" in their education. A sleeper hit is a phrase commonly used to describe media with little promotion yet has quality and has become a success. Essentially the respondent felt it was interesting to learn as a student, but it was, at the time, not something they thought they would apply.

Another graduate noted that learning Linux forensics on the course helped them as "a lot of people can get stumped as soon as [they] come in to contact with a Linux distribution, especially with [industry tools which don't] necessarily understand it"[56]. These graduates expressed that within their teams they, and very few colleagues in their teams, feel comfortable using Linux in investigations. In contrast, graduates also

[56] One graduate commented that an indication of a Linux file system in one version of a proprietary system is how the tool "will see unallocated space under a C: drive and a swap partition, and that is the only indication of a Linux file system".

expressed that Linux had been predominant in their course at CCCU where there was a need for more Windows and Mac Forensics, as this is what they encounter more within investigations[57]. Articulating that the general census among graduates at CCCU in previous years felt it was more aligned toward Linux forensics. When academics were asked about the content structure, a heavy presence of Linux on the course was due to its usefulness in getting the students to understand and apply the theory associated with how a computer system works, manually being able to carve out data, the ability to question tool outputs and conduct hands-on investigations when there are no recognised tools to turn to. Although, it was acknowledged by the academics at CCCU that more Windows and Mac forensics needed to be addressed.

While the presence of Linux was noted by some as heavy, one graduate with career outside of law enforcement identifies how the course gave greater opportunities beyond policing or private sector forensics; for example, networks or system administration. Mentioning that "people able to do Linux administration is not as much as people would like these days. So, even the basics [of Linux are] very beneficial". Suggesting that the fundamental learning within such courses allows contribution to areas beyond policing with the ability to provide professionals for related fields such as network, systems and security administrators who are involved in maintaining infrastructure, performance, security measures and resources. This may explain further the merge of digital forensics and cyber security among courses in UK HE.

Interestingly, of the 38 students who responded to rating the importance of Linux forensics (81.6%) and Linux as an Investigative tool (78.9%) frequency analysis (Appendix D – D.2.1) shows that the topics were rated of high importance for a digital forensics course[58]. Mac forensics, on the other hand, was rated slightly less important among students with a cumulative percentage of 73.7%. This is particularly thought-provoking as graduates and professionals note that Mac forensics "is becoming quite prolific now". Professionals interviewed in this study corroborated the rise in Mac devices for a digital forensic practitioner. One professional discussing that the rise of Apple devices in criminality and the challenges they provide investigators are not uncommon, acknowledging that:

> "6-7 years ago – if 10 people were arrested you would have seized one to two Apple Macs. Nowadays, I would say it is about a third of computers … The imaging side of them can be a challenge no doubt … With the new Apple filesystem coming it is going to be interesting to see what happens."

[57] Since, more Windows and Mac forensics have been introduced into the course at CCCU than graduates would have experienced.

[58] Where ratings Very Important and Important were cumulatively above 75%.

This was also voiced by graduates working with Apple Macs, who commented that "Mac forensics would have been useful, at least to touch on them, but it does become outdated quickly". While in their experience, it is an area where there are fewer practitioners with the training or skills to undertake these examinations. Voicing that:

> "Very few especially in this office have gone into Mac forensics. There are maybe three or four of us that know Linux. The idea of Mac forensics, how they are more popular and how each different OS stores things in different ways is important."

This point raises comments made by academics in this study as well as literature who note that practitioners need to be acquainted with multiple operating systems and their associated file systems (including Windows, Mac and Linux forensic analysis) to conduct effective digital investigations (Karie and Venter, 2014, p. 1235).

While addressing the need for more Windows and Mac artefact forensics at CCCU a graduate acknowledged having received some, stating: "I still use my notes from the lesson with a lecturer about PLIST files and … Macs; I still use my notes today because it was really useful." Another interviewee who spoke of notes and lectures detailed how they used their notes at the beginning of their career, but a couple of years in and they now find them "wholly inadequate". The researcher observed this was not due to inadequacy of the course nor its relevance, the interviewee put this down to the constant changes which practitioners must keep pace with. Drawing attention to the ever-changing discipline with the interviewee voicing: "if I looked at my notes from now in two years' time, I would say what are these I did not know anything". The alumnus recognises though they may not return to their course notes the underlying knowledge they have was learned on the course and ingrained in the work they accomplish. Though, the physical notes have become out-dated due to their experience[59].

6.5.5 Mobile Forensics

Academics highlight how the once "traditional here is the device, bag it and tag it" is now of much less focus and it's all about the mobile devices and tablets instead of the hard drives. Mobile forensics being an area which many of the academics noted industry seek from HE programmes. Though, chapter 2 highlights that many courses overlook 'Mobile Forensics' as terminology among module naming conventions and programme specifications, where available, do not provide in-depth course information about mobile

[59] Discussion about theory, practice and experience can be found in 6.7.

forensics on courses across the UK. Therefore, it is difficult to assess the inclusion of this as a topic, nor as an interest and skillset for common stakeholders. While it is noted that mobile device forensics is sought after, there is little evidence that suggests courses in the UK are effectively delivering education which addresses these needs nor the specific knowledge, skills and abilities shaped.

To gauge opinions of both students and graduates in this study, they were asked to consider mobile forensics as a topic, or the education they had received relating to mobile forensics. Of the students questioned, 38 recorded their view of importance for the topic where 60.5% felt that the topic as Very Important for a course in digital forensics. This result showed mobile forensics (a mean value of 4.45) fell in the top six topics rated by these students. Cumulatively, 86.8% felt the topic Very Important or Important; where, only one student felt the topic slightly important and four moderately important (Appendix D - D.2.1). While Table 6.3 (p.123) demonstrated that 14 students wished to master or felt mobile forensics as most important in the current industry.

Similarly, graduates from CCCU identified how the coverage of mobile technologies and forensic analysis of such devices on their course had been an asset. One alumnus expressed how the learning has been useful in situations where they "are forever explaining how cell sites work and cell towers to detectives". On the other hand a graduate who did not venture into the policing realm for digital forensics commented that the module which covered "mobile forensics … has not transferred to [their] current job", however, they were left with the feeling that "had [they] gone into forensics [they] think it would have been huge."

What is interesting to note are the experiences of one graduate who explained that most of their colleagues who joined or graduated at the same time but from different HEIs had far less hands-on experience and education surrounding mobile technologies on their degree course. Leaving the individual feeling that the course inclusivity of mobile forensics at CCCU had been an advantage for their career as a skillset sought after. Furthermore, graduates with mobile forensic analysis experience noted that mobile technologies and forensics was "always a good thing to learn as it is a big subject and it is an up and coming thing. Especially with chip-off forensics." While another reiterated that along with their placement experience, the mobile forensics at university provided them with a good base of knowledge and the use of standard industry tools to understand the need for, and use of, Chip-off forensics. A more destructive type of forensics for capturing data. The student acknowledged their third-year placement "working with law enforcement enticed [them] to complete a dissertation in Chip-off forensics". It was an area they considered which fell outside the learning on the course at CCCU and the remit of typical practices and procedures taught. The graduate recognised and reiterated the need for practitioners to be able to demonstrate how they are competent at carrying out tasks which fall beyond the standard principles yet, follow standard operating practices.

Inferring the need for not only experience but a critical and analytical mindset with the ability to problem solve and acquire investigative skills.

6.5.6 Live Data and Cloud Forensics

Equally graduates discussed how computing and forensic knowledge acquired on the course allowed them to transfer their investigative skills to Live data forensics. In recently devised frameworks less emphasis is placed on the need for live and cloud-based forensics where educational frameworks often broadly cover 'file system analysis' or 'networks and network forensics'. However, both the Cybersecurity Curricula Guidelines (Joint Task Force on Cybersecurity Education, 2017, p. 26) and the NICE Cybersecurity Workforce Framework (Newhouse *et al.*, 2017, p. 30,122) mention the need for live forensics. The latter, specifies live data forensics for one digital forensic role, a Cyber Defense Forensics Analyst and, is not common to professional roles classified under the umbrella of digital forensics (as shown in Appendix F - F.3).

One academic noted discussion with industry partners which distinguished gaps in graduate knowledge and skills which were "more technical" in areas such as Live data forensics. They express this as "something [which is] very difficult to implement in an academic setting". Live data forensics has not only been a weakness of education but has for many years presented challenges in the discipline/industry. It is a process dependent on analysing data there and then, an active forensics presence in what has largely been a reactive discipline. The process focuses on ascertaining what is happening on a system and a volatile process, far away from the traditional hard-drive forensics. Thus, the resources required to replicate such a set-up are costly and often impossible in an educational setting; again, reflecting the need for practical and wider disciplinary collaboration. Frequency analysis of student responses in this study show that students felt Live data forensics as highly important for a digital forensic course, where 50 percent of students rated the topic Very Important[60]. The topic fell into the top six subjects along with digital forensic tools, basic procedures, and mobile forensics.

As for the term 'Cloud' forensics, this is mentioned on far fewer occasions within the setting of digital forensics among the available educational frameworks. Newhouse *et al.* (2017, pp. 121–122) mention the need for 'Cloud' in relation to forensics for possessing skills using Virtual Machines (including "Amazon Elastic Compute Cloud", a web service providing compute capacity in the cloud). However forensically, cloud forensics is limited where 'Cloud' often covers services in the Cloud in terms of security, administration, and design models.

[60] Scale= Very Important, Important, Moderately Important, Slightly Important, Not Important at all.

One academic responded, "a big issue is cloud forensics". Testifying that the once "traditional here is the device, bag it and tag it" is now much less the focus and it's all about the mobile devices and tablets instead of the hard drives. Again, focus on the live data forensics arena, but it is also heavily weighted toward the need to extract "cloud and electronic traces" which are paramount in many investigations both forensic and security. In addition, it is "the element of encryption on top". Some of these topics are often covered in theory and not necessarily in practice among education institutions due to the prevalent challenges of implementation and assessment. Cryptography was mentioned in course analysis (chapter 2) on 11 occasions across module offerings. While, 76.9 percent of students questioned in this study felt cryptography to be highly important, two students felt the topic of on slight importance.

Alqahtany *et al.* (2016, p. 445) state that with a lack of and ill-prepared procedures towards tackling Cloud forensics as well as "few training materials [that] are available that could be utilized to educate investigators on the cloud-computing technology and cloud forensics procedures" that the need for training of "regulation, … tools and techniques, programming, networking [and] communications" are vital. This is still very true today and within most, if not all, educational environments.

The interviewee notes that "It's all changing, and we have to change our curriculum with that to reflect it" but acknowledges that this is not an easy task ahead. They would like to think that the academic discipline can keep abreast and flourish with the changes required but resourcing is the most excruciatingly difficult element to the everyday running of these courses as technologies advance.

6.5.7 Digital Forensic Tool Awareness

While all stakeholders in this chapter recognised that both proprietary and open source tools are important within the curriculum, their views on the inclusivity differed based on their own experiences. For example, many academics in this study noted that they use low level or open source tools to teach students aspects of digital forensics, where reliance on these is shown to be fruitful based on alumni comments and evaluation. Educators and course aims are far from providing students with rudimental skills and reliance on industry tools, but to gain a well-rounded understanding of critical workings and competences to be able to complete technical and complex problem-solving, analytical, and investigative tasks.

Though, digital forensic alumni in this study recognised that while these were paramount in their learning, they felt at CCCU, there was a need for more teaching with industry standard tools such as EnCase, X-Ways, XRY and other known tools[61]. Graduates expressed, while they would be expected to go on training for tool once acquiring a job, more experience on the course with the standard tools would have been fruitful

[61] This has since been addressed and awareness and use of these tools is included more in the current revised curriculum.

for job interviews and their initial start. Taking this into consideration alumni were able to recognise that while the use of these tools are essential to their everyday work, they must be able to understand the tools beyond this; for example, the inner workings of manual file carving. These attributes are essential to developing competences beyond the abilities of what is largely push-button forensics (James and Gladyshev, 2013a) and, particularly useful when explaining for example, in layman's terms, findings in an investigation. Students in this study were also asked to consider digital forensic tools and their importance on a course (both proprietary and open source tools were considered). Each was rated within the top six topics among student responses when rated 'Very Important'. 68.4 percent of students felt that proprietary digital forensics tools were very important and 63.2 percent for open source digital forensic tools.

6.5.8 Attitudinal Skillsets

One key belief alumnus in this study recognised and noted were expected of graduates could be categorised to attitudinal skills. In particular, the willingness to learn and put the time in to learn more than you are being taught within studies and within the professional role. This was epitomised by a statement from one graduate when asked if education can continue to keep up with industry demands;

> "I think as long as the students understand they don't know anywhere near enough yet and they are willing to learn more, then yes. To learn the basics is the key thing. I don't think the basics for forensics will ever change. Apart from when we get to live data extractions we have and essentially that is what we have now and encryption as well as the shear amount of data where we find ourselves previewing."

Furthermore, graduates identified the need for problem-solving skills, an analytical mindset, management skills (e.g., project, time and resource), communication skills (e.g., the ability to present in lay terms how they came to acquire data or how a particular concept works), through to writing skills beyond the traditional essay style such as, reports, witness statements and note-taking skills. These were also reiterated by academics in this study.

Final questions sought from students any further topics they considered important and, expect or consider is essential to support their future employability on their course and any final remarks. One student responded with "communication skills" as a topic/skill to consider within degree programmes. Both sociability and communication skills were mentioned in computing student responses (where there were an additional four computing students) and draw to attention the stereotypical belief that computing students are introvert, 'nerdy' and lack skills in social situations. E.g. they are often represented as people who prefer solitary intellectual interests and who are anxious toward interpersonal interactions. However, studies have suggested that there may in fact be an "overrepresentation of Introverts found [particularly] in the programming area" (Greathead, 2008, p. 10). Describing that introverts may be drawn to the discipline through applied skills and enjoyment rather than their potential to lack sociability (Greathead, 2008, p. 10). Buchler *et al.* (2018, p. 115) emphasise characteristics of an introvert linking to the skillsets of a cyber security professional and how these may help tackle the weakest link: humans, who are both the problem and solution in cyber security. Buchler *et al.* (2018) also epitomise the point that maintaining coherence, management, and coordination to effectively tackle cyber threats is paramount:

> "Managing the challenges of cybersecurity requires considerable interaction among teams of cyber analysts to monitor, report, and safeguard critical information technology around the 24-hour clock with shift-handoffs." (Buchler *et al.*, 2018, p. 116)

The same can be said for digital forensics practitioners where, to tackle challenges within the discipline interaction among teams, departments, stakeholders (including professionals and educators) needs to be an essential ingredient to managing and identifying future developments and successes.

One student picked up on the fact that the academic discipline suffers from, in some cases, a lack of practice. For example, highlighted above in areas such as network, mobile, cloud and live data forensics. While responses form stakeholders in this study have highlighted issues with awareness and contextualisation, one student noted that the "degree of knowledge" learned on a digital forensic course was important, they were left with the feeling that "there will be little experience" and therefore the "knowledge of the subject would be very important". Another felt, similarly, that "the ability to be a quick responder and apply practical knowledge to a situation solving problems efficiently" were attributes which would enhance and make an individual stand out among the crowd. These are key attributes which have been previously outlined by academics and graduates in this study to be important in demonstrating abilities and competence (e.g. technical or soft). Emphasis is not solely placed on the grade obtained from a university degree and, again, links to the balance between theory and practice as well as the need for softer attitudinal skills.

6.6 Experience, Education and Placements

> "I mean the day-to-day role is pretty much push-button forensics and it is only really the second stage where the stuff I learned at university really comes into its own especially when triaging, when you have to identify things and know what you are looking for. A lot of the files I am looking for etc., I have learnt [on-the-job] but the methods of getting to them I learned at uni." – CCCU DF Graduate

Experience is often a key criterion sought after in job descriptions for practitioner roles within digital forensics. Many roles consider applicants and expect between as little as 12 months' experience to 5 years' experience[62]. Particularly within policing advertisements length of experience are often concentrate on the persons experience within the discipline and/or law enforcement or other investigative organisations for roles such as Digital Forensics Investigators, Analysts and Technicians. Using criteria observed on job advertisements examples include:

- "we are looking for candidates with 12/18 months industry experience in either public or private sector"
- "knowledge and skills required in the role include previous experience in law enforcement/investigative organisations"
- "several years' experience as a Digital Forensics Practitioner"
- "3 years' experience in digital forensics"
- "preferred experience in digital forensics: 1 year"

One graduate noted there is the aspect of comprehensive and foundational understanding of computing required and which is important from university, however, they state:

> "for some reason employers expect experience. That is a thing they don't even seem to consider people at that level [graduates] will not have that. It is the chicken and the egg situation, and it is not something they seem to think about."

While one student went as far to say that the "industry is unwilling to employ without experience and [then] train up". Academics noted this is shifting slightly, where graduates are being employed in digital forensic units as assistants and how the range of practitioner roles available now extends beyond policing. Furthermore, the rise in cyber security roles and improved collaboration between industry and some academic institutions has helped. Graduates are therefore being employed in private sectors in corporate digital forensics. However, they acknowledge that there are far more digital forensics courses than previous years and so there are more students looking to start their career in the discipline.

Another graduate with several years' experience recognises that the shortfalls of most graduates tend to be the "lack of experience … [they] are working from the ground up and have to be moulded into how we [practitioner or business] work". This is a point which is reiterated in chapter 7 by professionals. It must be recognised that while this is a drawback, it would be the same for any job and fresh graduate. Education is a mechanism, as some graduates identified, to provide learners with the fundamental and grounding knowledge as well as essential skills and competences to initially flourish within the discipline. However,

[62] Information based on recent job advertisements within digital forensics within the UK, found on indeed.co.uk.

learning does not stop there and continues to be self-directed on-the-job, particularly where experience provides deeper and meaningful insight, skills, and competences.

While experience is an issue among fresh graduates and the increase in courses offered at HE, many now include placement modules or a year in industry to address some of the issues with industry's want for experience and issues with delivering real-life scenarios. An academic mentioned how placements in the early days of digital forensic programmes, i.e., the early 2000's, was challenging. With over a decade of experience in developing and delivering digital forensic courses, they noted that "undergraduate students came on [the course] specifically to become investigators at the end of it" where they "wanted to [be able] to walk out into a police department". However, the academic emphasises they "knew at the outset that [the students] weren't going to find these digital forensics placements". With more courses introduced, described as "a mushroom effect" by the participant, the likelihood of acquiring a placement in digital forensics became much slimmer.

The academic recollected how they had failed to address student expectations and "hadn't set the expectations right in the first year". Managing placement expectations meant more opportunities could be obtained beyond the policing environment, however, with only approximately "10 percent of students" finding a role in digital forensics. If this statistic is still true today, and one considers an average of 20-30 students on a course (based on results in chapter 2) that is just a handful of students who acquire a digital forensic placement. The academic also highlighted the success of placements on their course reached 100 percent when student expectations were managed, and opportunities were taken within the general computing and information technology sector. At the time, they observed cyber security was not an area any student would have considered. Now, as demonstrated in this study, cyber security is at the forefront of student career aspirations, based on students questioned and industry skills shortages.

While efforts to introduce placements have seen both drawbacks and successes, the potential number of practitioner roles may continue to grow while the number of undergraduates and postgraduates increase it is unknown whether there are chances for further placements in digital forensics and cyber security.

From the researcher's own observations in teaching, students are seeking more roles in cyber security than its digital forensic counterpart. Yet the challenges of obtaining these specific and security-heightened opportunities are still challenging as noted by many students studying at CCCU. Again, leaning toward professional experience in computing and information technology sector roles particularly focusing on networking and databases. Several reasons for these struggles and, to some degree, continuing struggles are the sensitivities of work within the digital forensic domain and the limitations of professional roles available. For example, security clearance in roles within policing, the sensitivity and confidentiality of evidential data and, overall, the nature of work and its mental and emotional affects. Contrasting views, however, of what is expected of such a graduate and what professionals would like to see is more hands-on experience and technical competencies as well as the potential for placement experiences.

Graduates identified that while there could have been greater levels of practical work, assignments provided problems and scenarios which were realistic. One graduate expressing if there had been more practical-based work it would have been beneficial, but they did not believe it would have provided much change to the position they are now; where, a year in industry or placement would have been most influential. “Even a month or two in industry to see how things work would have been ideal … working [in industry] is very different to university.” Experience by practicals and placements were highlighted by graduates interviewed on numerous occasions drawing to conclusion that there was a need for greater collaboration between academia and industry.

The literature has outlined teaching and learning using the delivery of scenario and problem-based learning approaches to recreate portions of investigations such as crime scene investigation and management, and court room scenarios and expert witness testimony. While pinpointing that assessments “were good to show certain portions” of an investigation, graduates form CCCU felt they could not always contextualise these portions. For example, one graduate mentioned, it “did chop and change a lot and [they were] not sure it was necessarily explained why… or did not really make sense in one long drip.” Where graduates noted they would have benefitted from experiencing a digital investigation in full during one year of their studies (i.e., their third year) which included all phases of a digital forensic investigation. Further noting that placement opportunities would have aided their learning and development.

Students in this study were asked to consider and rate the importance of education, training and experience within digital forensics. Based on the student level of study and their limited background in the IT sector, it is recognised by the researcher that the students questioned have little to no experience or training at this stage. Student responses show that high proportions of students felt all three were ‘Very Important, or ‘Important’ (Table 6.9, below). Though the results also highlight how students tend to view training of greater importance in digital forensics and/or cyber security. In immediate post-mortem results of the workshops students were asked about this response. Where discussions identified how students felt training would provide them with more specific skillsets for a role, rather than education which they felt, to some degree, provided them the theory and fundamentals and potentially not the skills to use a tool or a specific technique.

	Students	
Importance	Total n	(%)
Education		
Very Important	17	(43.59)
Important	16	(41.03)
Moderately Important	4	(10.26)
Slightly Important	2	(5.12)
Not Important at all	0	(0.0)
No Opinion	0	(0.0)
Total	39	(100.0)

	Students	
Importance	Total n	(%)
Training		
Very Important	28	(71.80)
Important	10	(25.64)
Moderately Important	1	(2.56)
Slightly Important	0	(0.0)
Not Important at all	0	(0.0)
No Opinion	0	(0.0)
Total	39	(100.0)

	Students	
Importance	Total n	(%)
Experience		
Very Important	23	(58.97)
Important	12	(30.77)
Moderately Important	3	(7.70)
Slightly Important	0	(0.00)
Not Important at all	1	(2.56)
No Opinion	0	(0.0)
Total	39	(100.0)

Table 6.9 – Students' View of the Importance of Education, Training and Experience in Digital Forensics and/or Cyber Security

This is supported by graduate and academic responses which draw on student awareness and abilities to contextualise these three situational learning environments. Academics and graduates also recognised that while students may not be extensively taught using standard industry tools throughout an entire curriculum, they will receive training and are expected to gain certification provided by companies/owners of the software on entry into digital forensic roles. Similarly to education, training for practitioners needs to align with knowledge and competences useful in the workplace and have impact on the performance in the workplace. The diverse coverage of training available, alike to higher education courses, can prove difficult to identify quality. Graduates noted mix views of training programmes, while overall they felt they were of good quality, some focused too much on how to use the tool and not enough content about topics, workings and essentially the fundamentals. This shows that while training courses are used to learn a specific task, they still need to include fundamental knowledge beyond click-button learning. One graduate exemplified this stating "training was useful and helped me learn how to use the tools more than we did at university… If I get called to court, I need to explain how things work and that is where the theory comes in useful". Graduates also recognised that the quality of teaching and impact on learning was different per educator or trainer and that "it doesn't matter how much you care about a subject, if you are bored you just won't learn as well". This also aligns with professional views discussed in chapter 7, where the need for graduates to possess a rather broad understanding, set of fundamentals and skillsets while not restricted to the use of a specific tools is essential.

6.7 The Requirement for Theory and Practice within Digital Forensics Education

Among participants in this chapter the preferred and ideal way of learning or teaching for digital forensics was identified to be heavily practical, where knowledge and skills could be applied to real-life scenarios. While practical learning stood out to be important, stakeholders were able to recognise the importance of theory and soft-skills for a digital forensic role. For example, students of this study (92% and 95% respectively) felt both theory and practice were important during their learning and development academically and, for the workplace (Table 6.10); some noting they are attributes required of a graduate.

	University A		University B			
Learning	Total n	(%)	Total n	(%)	Total n	(%)
Importance of Theory						
Yes	15	(93.75)	21	(90.5)	36	(92.31)
No	0	(0.0)	0	(0.0)	0	(0.0)
Maybe	1	(6.25)	2	(9.5)	3	(7.69)
Total	16	(100.0)	23	(100.0)	39	(100.0)
Importance of Soft Skills						
Yes	14	(87.5)	23	(100.0)	37	(94.87)
No	2	(12.5)	0	(0.0)	2	(5.13)
Maybe	0	(0.0)	0	(0.0)	0	(0.0)
Total	16	(100.0)	23	(100.0)	39	(100.0)

Table 6.10 – Students' View of Importance in Learning Theory and Soft-Skills

This brings about the discussion of whether courses provide enough practical learning as well as theoretical knowledge and the clarity of their course content to a range of stakeholders. Graduates polled suggested that their course did not have much practical at the time when they studied[63] and that the "theory gave [them] the understanding to do the practical [where] a lot of the practical stuff is where a lot of the tools do it for you but because [they] learnt the theory, [they] know why the tools do what they do". This suggests that learning the theory provides students with an understanding of what happens beyond a tool interface. One respondent highlighted that there needs to be a "50/50 ration on the backbone concepts and how to use the tools" affirming that

> "both are necessary; if the tool does not work, you need to know why. Especially if you are in this type of job you need to be able to explain to a jury why it did not work, and it

[63] Time periods of study started in 2011 and ended in 2017; graduates completed the course within three years.

> is a lot easier if you can actually argue your point without looking at Google. You tend to have more standing at court if you know what you are talking about."

Arguing that this way of learning therefore provided these graduates with the mindset to question the tools and what they produce due to their understanding of the workings of devices and data storage concepts. Although, one graduate stated that "the little workshops [they] did with file carving etc., were great but [they] don't necessarily think [they] needed to do them practically as [they] had the theory from the programming in other lectures." Expressing that some time might have been better spent elsewhere "especially as … a lot of tools do it". They recognised these exercises as "good to cement the theory" but felt that concentration could have been turned to more pertinent areas such as, evidence bagging and tagging, imaging hard drives, working with dead laptops and taking them apart through to more complex data analysis such as "work on Torrents … to have experience of extracting that in [well-known industry used tools] and analysing would have been ideal."

Other academics have stated they feel that this is not always fruitful and does not define a digital forensic degree. However, this academic describes that the computing fundamentals are essential and that they are still happy for these students to be learning mathematics, as again they are key skills for computing. Academics identified that they do little mathematics on their courses, where it is often "some really simple stuff". This may be due to what one academic acknowledges "that whenever mathematics is mentioned in a classroom setting half the class switch off".

6.8 Balancing Skills and Subjects Sought After

Balancing expectations and views within the educational setting does not only take into account students and graduates. In fact, academics have to consider the wider stakeholders such as public and professional views, requirements and expectations. It becomes a matter of balancing these to create an education which provides learners with the most crucial and beneficial skills to set them up for their new career yet benefit the industry. One academic accentuates the fact that a course will not meet every industry need and that there are some requirements that a course must meet more than others. Where they state they "do not believe that a degree programme should be designed to meet a particular industry need as we [the academics] have to offset the breadth of material that students should be engaged with as well as the technical training they should be doing."

Academics discussed with the researcher how they went to industry "for the gaps or bits [they] were doing too much of, or bits [they were] miss[ing]" noting that there is "a balance, a trade off … You can't do everything they want but you can sort of make sure you have got most of the skills." Another academic noted that how they “wouldn’t listen to everything they [industry] say and jump as high as they say” this was due to the observation that if some industries within digital forensics had their way “they would just turn everything into training because they want people to do processes and they will perhaps be focused or interested in their particular sector. Whereas we [academics] might be covering several sectors”. This was a theme recursive of interviews with all academics where a need to balance what industry want from academia and what academia can provide is paramount to an effective course and curricula.

Furthermore, it was mentioned by another academic that bias and experience of professionals who they seek advice from must be considered. Educators “have to recognise there is a divergence of views among professionals in terms of what they want.” More so, the expectations and requirements will differ based on size and domain of the business seeking digital forensics practitioners. Therefore taking into consideration the range of requirements, a balance and alignment of a course with a broad range of fundamentals are necessary, correlating with the notion of a digital forensic investigator having the fundamental skills within computing and forensic principles to apply in a multitude of roles and investigations.

When a programme is due for review there are several stages which take place, however, an important part and involvement in the review is the cooperation of an industry panel (e.g. several professionals within the discipline) who are willing to look at the programme and make suggestions whilst considering the objectives and goals of the course and expectations they would have for a course and student graduating with the degree. Furthermore, employers can provide specialist input into the course and assessment processes with opinions before academics agree on course attributes and content.

6.9 Higher Education: Can it, and does it continue to meet industry needs?

An interest of this research looked to identify how the stakeholders felt about academia meeting and addressing industry needs. Interestingly, academics showed mixed views for example, one academic noted how they felt “some of the universities do it really well, but a lot of universities where they have put the odd module in and states they are doing forensics (playing a little bit of lip service) are not. … There is quite the difference.” Others responded “no” more can be done to meet the needs of industry while keeping in mind a range of theoretical underpinnings students must receive.

Other respondents felt that academia could keep pace with the industry needs but only through more collaboration. Academics highlighted that they have improved collaboration with practitioners over the years, but more work is needed. This is something reiterated by professionals in chapter 7. One problem of continuing digital forensics programmes in academia is whether there is potential for the problem of cost being too much for institutions, one academic respondent expressed ‘yes’. They noted that it was a matter of strategy in the current climate of the course continuing as it aligned to thematic areas introduced across the university. These experiences have also been felt at CCCU for several years, where the challenges behind the delivery of such a course are often the higher costs of running an effective programme to meet the needs of student learning and in the long run employability.

6.10 Key Themes from the Chapter

There are several key themes that have been discussed within this chapter from the viewpoint of stakeholder groups (i.e. students, graduates, and academics). Figure 6.6[64] demonstrates the four key themes which converge form the repsonses analysed.

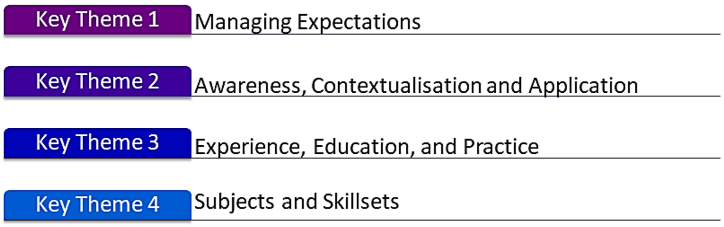


Figure 6.6 – Key Themes in from Student, Graduate, and Academic Responses

With each key theme there are crossovers and independencies. For example, the first theme considers the management of expectations. As indicated in this research, this is a task for academics who must manage the expectations of potential students, current students, and also graduates. Management of expectations for these stakeholders include topics of study, practical value of scenarios, tasks and application of their learning to the jobs they may explore. However, managing expectations is not only relvant for academics and their students, but also academics and industry partners. Involvement of industry in the value of a course, and of a graduate is something this study has explored, and found that academics must attempt to manage the expectations of industry partners as well with regards to what knowledge, skills, and competences industry expect of a graduate on completion of their studies, and what they expect to see in a course which must target multiple job roles within the digital forensic domain. Therefore, the management of expectations converges with the awareness, contextualisation, and application of learning on behalf of the students. This focuses on the student's ability to recognise why they are learning specific topics and how the knowledge applies (theory-practice links) to the common digital forensic roles and tasks. Improvement will be seen in the contextualisation and application of their learning with far greater practice and experience. Some practice will be evident through practical learning on a course, however, experience on-the-job will allow graduates to become more effective over time and application of their knowledge

[64] An extended version of this diagram can be found in Appendix: .

with real-world tasks. Themes 1, 2 and 3 also converge with theme 4: subjects and skills. The value of the subjects taught on a course may only be recognisable on exit of a course with experience and awareness of the role with the ability to contextualise the materials and apply them on-the-job. Similarly, the skills and competences gained will be dependent on the job role, activities, and experience a student collects over time. The output of all the independencies would make for a more effective graduate over time. What is essential are the fundamental knowledge and skills which a student and, by extension, a graduate have gained during the course and their ability to put these into context and apply them effectively.

6.11 Summary

This chapter has focused on the views of three main stakeholders within this study thematising experience, views, and ideals from participants. Results have discussed challenges and issues with awareness as well as critical subjects for a curriculum and for practitioners to be accustomed with. Topics highlighted have included fundamentals through to topics of much more interest and necessity among course curricula due to technological developments such as, mobile, network, live data, and cloud forensics. Another main result from the three stakeholders looked upon in this chapter, and similarly, observed by the researcher through action research in teaching digital forensics, has reflected how students within digital forensics and cyber security today are unable to see how their learning may be useful in the real-life role of a practitioner. These are results which are drawn on further in chapter 9 where this thesis provides insight to the range of stakeholder views narrated within this research.

7. Digital Forensics Education: Insight and Experiences from Professionals

Introduction

This chapter focuses on the views of professionals as stakeholders looking at what is required and makes an effective digital forensics practitioner. Responses from professionals draw on perceived requirements of a graduate entering the professional discipline and the challenges of education and training in effort to approach the main research questions of this study to understand the delivery of education and training as well as perceived positives and short comings through the acuity of the professionals. This chapter takes into consideration previous stakeholder views depicted in chapter 6, using these to identify similarities and differences to identify the most pertinent of expectations, topics, knowledge, skills, and competence to make an effective education and practitioner.

7.1 Recap on the Method

Within this chapter, questionnaires and semi-structured interviews were conducted, as discussed in section 4.4 of this study. Participants were selected through convenience sampling (section 4.4.6.1) where interviews were conducted with known individuals and a questionnaire spread via social networks and email. Pre-determined/guiding sets of questions were used to promote discussions in areas such as learning, training, topics, skillsets, and challenges. The information gained were coded where possible using thematic analysis and used to establish common themes among responses from participants not only within the professional stakeholder groups but across all stakeholders.

7.1.1 Rationale and Themes of Questions for Industry Professionals

Based on the research conducted in chapters 2 and 3, and the research questions for the overall study several questions were determined for the interviews and questionnaires with professional participants. This section discusses the general areas of the questions posed, their importance, focus and rationale.

Stakeholder Group	**Question Themes**[65]
Professionals	- professional's background, role, and responsibilities - experiences with education and training in digital forensics - thoughts on current education/training offerings in the UK - education/training keeping pace with industry and its demands - collaboration with industry and academia - graduate skills and experiences working with graduates - education, training, and experience - skills-shortages in the current industry and tackling these - educational frameworks in the field of digital forensics - progression of digital forensics industry

The rationale behind the themes of the questions were to capture views and experiences of the very people who work within digital forensics. The idea being to not only collect information about their own experiences with education and/or training, but also with other individuals such as students and graduates. Ideally, the professionals would be able to identify key knowledge, skills, and competences required in a job in digital forensics. They may also be able to identify the shortcomings of current/previous alumni and enhancements that could be made across education and industry to facilitate effective digital forensics educations from the viewpoint of industry as a stakeholder group. With a lack of views portrayed from such stakeholders in existing research the questions and themes were drawn using current literature and action research (e.g., the identification of a lack of professionals as academics, identification that it is a resource demanding subject, the idea that the subject has to keep pace with fast and ever-changing technologies and so on).

7.2 The Professionals as Participants

A total of 30 industry professionals completed an anonymous questionnaire, and 3 professional interviews were conducted with individuals who responded to a call using convenience sampling methods (discussed in chapter 4). Of the 30 questionnaire participants, just three identified as female. Respondents to the questionnaire included individuals from European partners. Interviews saw participants based in the United Kingdom, with ranging backgrounds and length of experience (depicted in Table 7.1). It is important to identify that the questionnaire was anonymous and therefore there is a possibility that those interviewed may have also taken part in the questionnaire, however, this cannot be affirmed and may be distinct from the questionnaire. While this is possible, the interviews were in-depth and gleaned more information from individuals about their experiences, views, and opinions, and thus duplication would have little impact on

[65] Example questions can be found in Appendix A - A.4.

this study considering thematic analysis and the use of data triangulation and saturation. The questionnaire or interviews were not targeted and therefore 'professionals' in this context are not defined by any boundaries.

Participants (p) – Interviews

Target Group	ID	Occupation or Industry	Gender	Years' Experience*	Previous Role** Years' Experience	Interview Duration and Site
Professionals (P)	P1	Public Sector	m	14 years	Total years' experience = 17	1 hour 20 mins - Online
	P2	Corporate	m	3 years	Total years' experience = 15 ½	1 hour - R-Campus
	P3	Consultancy	m	2 years	Total years' experience = 20	1 hour 30 mins - Homebased

R- = Researcher I- = Interviewee
*Current Role **Previous Roles Combined

Table 7.1 – Academic and Graduate Interview Participants, Locations and Duration

The meaning of professionals in this study is a synonym for those working within the field. The study was not restricted by whether or not someone held an industry relevant certifications or qualifications as this is a larger and diverging debate within digital forensics, highlighted in section 3.2.1. Due to issues when gaining access to industry professionals, as described in section 4.4.6, boundaries were not set specifically to specific roles in digital forensics, and the potential to include cyber security professionals was left open due to the shift in educational practice at undergraduate level seen in chapter 2 and 3. An open call for participants was included on digital forensic forums, social media and university publications using convenience methods where many of the contacts of the researcher and colleagues would have been working within the field of digital forensics. Furthermore, specific calls to digital forensic companies, law enforcement units and others were sent via email or website communication forms to gain access to a wider audience. Examples of job titles listed by participants are included in Table 7.2 and demonstrate that the participants are largely centred in the field of digital forensics.

Job Titles
Network Security Engineer
Security Administrator
IR and DevOps
Forensic Consultant
DFIR Consultant
Digital Forensic Analyst
Digital Forensic Examiner
Digital Forensics Investigator
Computer Forensic Investigator
Mobile Phone Examiner
eForensic Investigator
Digital Intelligence and Investigations
Forensic Manager

Table 7.2 – Example Professional Participant Job Titles

7.2.1 Professional Participants Expertise

To understand the level of experience and background of each professional, the questionnaire asked several questions targeting their employment e.g., sector, length of service, job title, technical specialism as well as qualifications. This data was collected similarly to a pre-information sheet utilised when interviewing. Responses found the public sector to be the most popular area of employment of those polled, where many professionals were employed within law enforcement/policing. Job roles ranged from Detective Inspectors in Intelligence and Investigations and Digital Forensic Manager through to Network and Security Engineer and Forensic or Security Analysts. Table B.4.1 in Appendix B demonstrates the demographic of professionals who participated in the questionnaire, identifying by gender several key data e.g., area of employment, length of experience, qualifications and input when employing new colleagues.

When asked to identify their own area of expertise, several topics such as network security and forensics, computer/mobile examinations, Operating Systems (OS) forensics, e-forensics, sandbox analysis tools, encryption, incident response, malware, cybercrime, cyber security, policing tactics and wet forensics were highlighted. Many of these topics have been mentioned previously within this study either inclusive in digital forensics and cyber security degrees or the need for further coverage. Of the five professionals who identified their sector of employment to be digital forensics, digital investigator/examiner and e-Forensic Investigator were highlighted as job titles. It can be surmised that these professionals may work within law enforcement/policing, demonstrating close boundaries in the categorisation of job roles. However, assumptions cannot be made as to whether these professionals are based in law enforcement or the private sector, so have therefore been kept separate to other related groupings.

Table B.4.1 (Appendix B) further demonstrates the level of expertise through a range of years' experience. Results show that nearly 47 percent of professionals had a relatively short time based in industry with 0-5 years, followed by 30 percent who held 6-10 years, 17 percent with 11-15 years and nearly 7 percent with 16 or more years' experience. Of the 30 respondents, 19 noted having a qualification from higher education related to digital forensics and/or cyber security. This left 11 respondents (36.7 percent) answering no to "Have you completed any form of higher education related to digital forensics and/or cyber security?"

Figure 7.1 depicts the correlation between years' experience and whether the participants, of the questionnaire, have completed any form of HE qualification related to digital forensics and/or cyber security. The radar diagram demonstrates most respondents who had fewer years' experience were more likely to have completed a related form of higher education. Whereas those who responded no, often had a greater number of years' experience and no form of related higher education in digital forensics or cyber security. It should be noted, that it is possible these professionals have experienced higher education from a different subject or training scenario. In other circumstances, individuals may have worked to such roles through on-the-job training. As discussed previously, on-the-job training for computer forensics, was at the forefront of professional development in its earliest incarnation within the public sector.

To assess professional views on what makes an effective practitioner/graduate and their contributions when hiring new employees, respondents were asked a simple 'yes' (n=12), 'no' (n=11) or 'sometimes' (n=7) multiple choice question for their involvement. Of the interview participants, all three were male, with between 15- and 20-years' experience within digital forensics and information security ranging from public and private sectors. Two of the participants had some input in hiring new employees, and all three had experience of presenting to undergraduate students on multiple occasions. Within this chapter, any responses from academics interviewed who held previous professional experience within either discipline will also be drawn upon.

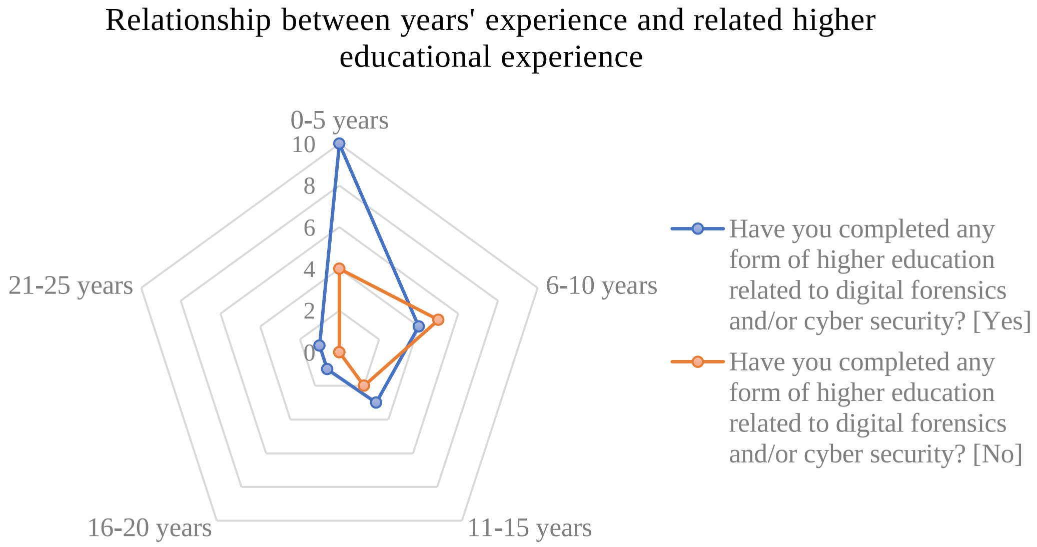


Figure 7.1 – Professionals experience and related higher educational qualification completed

7.3 Focus and Results

This section looks to responses from participants through questionnaire and interviews, highlighting key topics of interest, expectations, and experiences as well as views within digital forensics and/or cyber security relating to academia, training and graduates. Individuals were asked to express their views on issues they felt were current of educational programmes and/or graduates and what they would include or do differently on such HE courses. With all participants specialising in mainly digital forensics, these views have been collated within the section for discussion, where issues and expectations are discussed in tandem.

Furthermore, participants were asked a range of questions to identify their views on what they would expect to see from a graduate with a digital forensics/cyber security degree. Questions included identifying skill shortages within the discipline, be it technical or soft skills. Participants were also asked to identify topics that they would expect to have been covered within education and for graduates to understand. To supplement, this identification of general skills shortages in the industry was used as a pointer for discussion of developments that might need to take place with curriculum and skills delivered through graduates. Responses from these questions are discussed in section 7.3.2.

What should be noted at this stage is the views of these participants are based upon experience within roles in digital forensics or cyber security and thus their opinions will differ based on specialism, length of experience and own experiences and attitudes toward several influenceable factors.

7.3.1 The view of professionals: issues with, and suggestions for, current higher education programmes and/or graduates

As Hénard and Roseveare (2012, p. 8) state "graduates are entering a world of employment that is characterised by greater uncertainty, speed, risk, complexity and interdisciplinary working." The requirements of graduates and need for quality teaching and training is ever growing. For highly technical and scientific disciplines, the need to keep pace and provide quality is even more so. With the professional experience of respondents identified (i.e. years' experience and job role) discovering their own experiences and views, within and, of higher education and training were to be deliberated.

To approach the questions *what makes an effective digital forensic practitioner?* and *what are the perceived requirements of an effective digital forensic practitioner?* on behalf of professionals themselves, firstly issues were identified they felt exist with current digital forensics and cyber security education programmes and their graduates. The professionals were open regarding issues they had discovered where a key focus was central to fundamental understanding and awareness, real-life hands on approaches and practical experiences.

7.3.1.1 The disparity of courses offered across the UK and Europe

The discipline of digital forensics education is still niche for many countries as highlighted within the literature review. One European respondent recalls how "this type of education is very new" in their country and responds that they "have had Master's study in forensics for 3 years … [yet, they] do not have [any other] 'higher education' in this field". Another respondent accounts that such education is "not widely spread, nor is there much advertisement for it in most ICT bachelor schools."

On the contrary within the UK, there are several courses as depicted in chapter 2; several practitioners expressed that the various courses on offer in the UK can cause problems for employers. One professional interviewee expresses that the trouble they have is not knowing what is exactly taught on the courses. They go further to discuss some challenges faced in academia where, from what they have heard, "the biggest challenge in academia has at the moment … [to be] the variance between standards of a degree course [where,] there seems to be quite a wide disparity between them." They continue by noting "and that is natural with any course I guess."

This point is very akin to the problems faced by the applicants to universities who are looking to pursue such a career. Each degree is different, and each covers a multitude of topics and modules; however, as noted in chapter 2 the briefings, documentations and marketing do not often provide for a coherent understanding, perception or unwrapping of the course from a first look.

The professional identifies that they browsed curriculums which are on various university websites and "they all kind of read quite well" but the problem they have is they do not get an indication through these regarding "how much they [, the students] get taught about each … specific area". The participant notes that for some aspects of the discipline it "takes weeks to be taught effectively, and if they are only taught and covered over a couple of days, it is only giving them an awareness". Yet, other areas of the discipline take years of experience before they can truly master the know-how and practical problem-solving and hands-on skills.

What can also be linked with these points is an observation recalled by one interviewee and how they felt,

> "one of the problems [they] have seen over the years is that it certainly became fashionable to offer a forensics course without necessarily having the people in place who could actually teach the forensics course."

Similarly, a questionnaire respondent with 6-10 years' experience working as a security analyst vocalised the same view, stating what they would include or do differently at HE involved "more hands on, less academia [and] good teachers with experience, less paper-pushers." This does not allude to all courses nor academics and links to one of many problems with the general lack of resources (technical, soft or staffing) as well as little collaboration there is among academia, training and industry to harness the best learning and development toward the largely fundamental requirements in today's age of both disciplines. Authors such as Karie and Venter (2015) identify challenges with the lack of qualified personnel and "forensic knowledge reuse among personnel" focussing on operational and investigating personnel more so than the educators. Challenges with education for professionals may be linked with the "time-consuming and overwhelming [nature and how] one can easily be a full-time student for many years, and still not know everything." This is something which graduates note students must be aware of. Furthermore, one professional noted how education can "take resources from the production line in work with constant education, [however,] education which is highly needed to do a good and sound job." Challenges with skilled educators on the other hand are accompanied by aspects such as resourcing, training, and delivery of a curriculum which is broad yet in-depth to provide for multiple professions within the discipline.

Another view presented by a professional consultant with 21-25 years' experience focused to the "require[ment] for an appropriate apprenticeship working environment". At the time of writing there are very few digital forensics apprentice schemes; there are a number of cyber security schemes which involve an element of digital forensics such as GCHQ, BT and the National Grid. Another participant expressed that they felt the issues with current links between the industry and higher education or training course providers were that there were "not enough apprenticeships and exposure to the social skills and client pressures." Again, this highlights the strong views of participants that the need for experience either through "some form of apprenticeship/work experience would be beneficial." Apprenticeship schemes may in the future be useful for educating and training employees within the profession in the future, however, considerations must be made to identify and address current challenges with collaboration and placements.

Much of what the professional respondents discussed were coded down to experience of the graduates, variance among course curricula and resources. These have been common threads throughout this thesis where experience has been a fundamental and strong factor and influencer.

7.3.1.2 Shortfalls of HE courses in delivering the fundamentals and skills shortages of graduates

> "Certainly, [in my last role] if we got applications from people who didn't display a background and no interest in computing then we were not keen."
>
> —Professional Interviewee Response

Although the above statement seems obvious in nature it is quite telling of situations experienced over the years as heard from several participants. This participant, with over 15 years' experience, discussed how they had experienced interviewing lots of potential employees, including graduates, and "you don't want someone who is going to Parrot answers". Recollecting experience running recruitment exercises, of which they were involved in eight or nine where, "you could spot the groups from particular universities as they gave the same answers". They stated they employed one individual as "they were outstanding". Responding again that "you want someone who is not just going to regurgitate what they have learned. They should be going away and doing their own research to find stuff out."

Two interviewees discussed how they prefer to employ people who show a passion not only for digital forensics but for computing in general. Where having applicants who have "built [their] own machines, have a little network at home, [and] do this that and the other and so some programming in [their] spare time … [shows] some real interest."

One asserting how they

> "would prefer to employ someone who has been taking a computer apart since the age of four and programming their entire life, rather than someone who decided at the last minute that they were going to do a degree in digital forensics and three years later has their degree."

The respondent further discusses how the two people can be very different and how this can often present different mindsets. One of these interviewees draws attention to "two simple little things but they stood out for [them as an employer]". They comment that "a thing that always stands out in [their] memory are always the questions that [they] would ask about the ACPO guidelines." The ACPO guidelines are a practitioner's lesson 101 or first aid basic principles. The interviewee describes recruitment exercises at the time for successful applicants passed the sifting stage included multiple-choice examination as well as essay-based questions. One question focused on the ACPO guidelines where the potential employers "used to get sets of answers per university". The other would be to throw a question in asking the applicants "what is your interpretation of the term indecent image?". This, a strong and potentially an unsettling question for many but, in a digital forensic role would get "people … thinking about the stuff that they might be dealing with, so it was not a shock for them … again, you had the same stock answer depending on the university they attended." The interviewee recalled how "rather than a vanilla answer, you would look for people to say how they would cope and examples of support … people who were able to think about this and are prepared/understand."

The issues of fundamental understanding and awareness was also addressed by one academic interviewee with experience as both a professional and academic who discussed how their wealth of experience over the years allowed them to observe a multitude of shortcomings of graduates and academia. The respondent notes that only a few years back they felt that "the low-level technical skills … [were not] that detailed" on some courses. They give the example that some graduates you could sit down and ask to do a fundamental task such as imaging a drive and the first problem would be "they haven't used or seen that particular tool before, as it might be one of many industry-based tools". Accepting that the experience many graduates had was using "dd in Linux because that was a lot of what academia was doing" at the time. The participant recollected how they would "introduce [a graduate or student] to the tool and ask them about some basics, low-level stuff like partition tables or file system limits and they would be a bit sketchy on [the details]".

Academics in this study have noted that they often turn to open-source tools and Linux based learning to educate the students at a much lower level and assumed often due to challenging resourcing. However, what most academics have distinguished now are they are using industry-based tools more in the curriculum, so students get a much wider understanding and delivery of the tools alongside those previously harnessed within the curriculum. Although, the participant did note the importance of Linux. The importance of Linux was also highlighted by graduates in this study as an essential element of learning for their future roles. Reply from one professional questionnaire respondent identifies that balance that is required between industry known tools and those featuring an open source nature stating an issue with some university courses is that they

> "can often use forensic programs that do a lot of the hard work for you using scripts (like EnCase) without giving much of a background unless you went on a EnCase-issued training course. Vendor neutral approach means a wider range of forensic methods are shown."

The interviewee above mentioned also recalls that, although their experience working with graduates was limited, they did have some experience of guest lecturing at a few universities, and now working as an academic, where they found "familiarity with looking at Hexadecimal displays, grids of Hex and thinking in terms of offsets" was a shortcoming in what they witnessed. They talked about the fact that students nor graduates or even industry professionals are "expected to know the decimal value of a hex number, other than the common ones, but they do expect you to be able to look at the output of the tool or raw data and work your way around that data without a nice pretty tool that tells you this is where you are". Thus, the ability to "verify and validate a tool and check the raw data from first principles [a key element within investigations]. So, [students and graduates] need to [be able to] navigate hex."

The focal point here being the basic principles and procedures, the low-level technical skills and the practical element within education. The participant continues to describe how labs at a minimum need to take "students through basics, going back to first principles, reading hex, displays or reading partition tables or finding internet history files and decoding them." A theoretical and practical approach incorporated to enable students to apply the knowledge they are gaining. The participant notes that since joining academia they have made changes to a programme, adding more practical elements. Acknowledging, that although "students are all different" and learn in different ways, "at the end of the day from a practitioner point of view, going into industry and not being able to apply that knowledge puts you at a disadvantage regardless of what tool you use." They continue to make the point that although the students need to be able to use the tools, they need to have learnt and applied several tools for more than a few weeks coverage across their studies. It is not the tools that should matter but the understanding of the what and why, and "that they are looking for a partition table and they see the raw data and know how to navigate it and know what a partition table is and they know the rules as to how many partitions you can have [and so on]."

Another interviewee observes a similar point, recalling their own experiences having delivered presentations to students on the brink of graduating and having witnessed "blank faces … when talking more loosely and commonly about industry used tools". The participant notes that "the lack of understanding sometimes can be a bit of a worry, in [their] opinion." The interviewee recognises that "variance" plays a part here in what is expected based on their own and other peoples' experiences and views.

Looking more closely at the point, the participant recalls of challenges with standards of graduates and courses within academia, they informally discuss anecdotal evidence where they have heard examples such as, "oh yeah I came away three years after and I didn't know much more than when I started" in comparison to other examples where "they walk out like oh yeah production machine robots and they can do everything". This highlights the "trouble from an employer's point of view" where it enhances the case of "what university did you go to? … which becomes more relevant." However, as seen from the view of some graduates (chapter 6) who graduated from CCCU, it can often be the case that the student does not recognise what and why they have learned something. It is not until application of taught subject on-the-job that some alumni truly recognise the relevancy of topics taught in higher education, where they can appreciate their use. Again, focusing back on the element of practice and experience, where it will often take what they have been taught and learned applied within a professional setting for a length of time before they truly grasp the necessity for some topics (similarly discussed in chapter 6).

These points raise awareness of the importance and impact an individual's (e.g. student or graduate) own perceptions of their learning and course can have on their resilience and employability. The way which alumni present themselves and their course, the grounding and enthusiasm they have, as well as their fundamental understandings may, arguably, be an influencer of, and provide reasoning for, the need of greater experience in most digital forensic roles.

These participants very much highlight that all graduates should depart their degree with the necessary core skills of the discipline and the skills to recollect and apply the knowledge they have obtained to practical and real-life scenarios. The difference to a core skills training programme comes from the aim in an educational environment to "not just tell them how things work but … get them to think critically about it and critique things [and evaluate things more] which you don't do on a training course [where] you are told what buttons to press, what to click and how to do something", as discussed by a professional now turned academic.

Respondents to the questionnaire also highlight how they would expect a graduate to have a broad range of skills with focus on an understanding of a range of operating and file systems, servers, networking and communications as well as a good understanding of a range of devices (not solely computers). These are epitomised by one respondent when asked "What do you expect to see from a graduate with a digital forensics/cyber security degree?";

> "Knowledge of Linux, basic theory about computers (build-up, binary/hex), the forensic process, knowledge of some forensic open source tools (like TSK), imaging and "basic" artefacts. Basic analysis knowledge, but I know that analysis skills comes from experience/working with analysis, so I would not expect them to be ready to perform a complete analysis on Day 1."

The previous interviewee also touches upon Linux Forensics identifying that they would not remove this entirely from courses and that it is important, but they discuss how within industry a "Linux machine [is often only used] for certain special cases but everyone works in Windows" in the digital forensics environment. Again, focusing on the low-level technical concepts the interviewee discusses the importance of being able to do "fundamental file carving, data recovery, decoding file systems, reverse engineering, Internet history, finding an SQLite database and pulling stuff out by hand in a Windows environment because that in practice, pretty much, exclusively happens in Windows in the practitioner world." A shift from the heavy Linux hands-on approach many universities were opting for several years back. Implying that there is a need for courses to have at least a 50/50 split across the three-year degrees to include both Windows and Linux forensics.

Participants from the online questionnaire recognise that there is a lack of Linux file system and forensic knowledge, or an expectation of a graduate to have learnt this on their degree. Linux was mentioned by 12 of the participants across 18 instances. Responses saw, for example, one respondent with 0-5 years' experience of conducting computer examinations state that "Linux/Mac knowledge is lacking certainly, most people stick with Windows as that is what they know and have understood." Another respondent with the same length of experience and role highlights "you don't need to know everything about Linux, but an awareness is a good start." Responses voiced pointed to knowledge, skills and abilities toward the use of Linux as a tool in forensics and cyber security tasks, knowledge of Linux and forensic analysis of "Linux [and] Apple file/operating systems".

Linux is mentioned in current cyber security frameworks (those discussed in section 3.2.3) under the remit of specialised categories such as Systems Administration and Operating Systems, although their applicability here is very much centred on fundamentals for cyber security roles as opposed to digital forensics (Joint Task Force on Cybersecurity Education, 2017; NCSC, 2017b; Newhouse *et al.*, 2017). One role identified under the US National Initiative for Cybersecurity Education Framework – Cyber Defense Forensics Analyst does mention the ability "to conduct forensic analysis in and for both Windows and Unix/Linux environments" (Newhouse *et al.*, 2017, p. 89), supporting the claims of professionals within this study.

7.3.1.3 The issues with, and the need for, experience

> "Experience every day of the week and twice on Sunday!"
>
> – Professional Interview Participant

A Bachelor's degree, once a differentiator, is now a standard request for any job, particularly in specialist areas, where a relevant and related degree is necessary. However, more and more, experience is seen as an accompanying requirement in many job specifications, most notably in technically heavy subject disciplines. Looking at digital and cyber related job advertisements the length and breadth of experience differs, with some looking for a minimum of two years required experience in investigations and/or a previous role in law enforcement, through to others looking for three to four years' experience. Thus, work-based learning (e.g. a placement, internship or work-based volunteering) can become highly valuable to a graduate's employability (Anderson *et al.*, 2006; Andrews and Higson, 2008; Bennett *et al.*, 2008).

Previous findings in this thesis discovered that academics acknowledged and felt that there has been progress made within digital forensics and cyber security with hands-on learning approaches such as Problem-based and Game-based learning, in addition to placements and the delivery of industry masterclasses. However, academics interviewed recognise that there is still much work in promoting collaboration, development and real-life experience which should be sought after within such educations. Similarly, Lowden *et al.*, (2011) also note that progress has been made in HEIs in response to the growing need for experience in obtaining a job and producing an effective graduate.

Although, there is still much promoting, understanding and development required among HEIs, industry partners and graduates. Where, Lowden *et al.* (2011) discuss several tensions and deficit skills due to conflicts of interests and boundaries among stakeholders. Lowden *et al.*, (2011) identify challenges in collaboration and funding between employers and educational establishments, often due to employers "prefer[ing] to train employees when they started work rather than provide universities with money to do this beforehand". This study drew on this common understanding that there is more which can be done to foster and promote greater employability within higher education, particularly focusing on the skills deficit in digital forensics and collaboration among HEIs and industry partners in the eyes of professionals.

With this in mind, one questionnaire participant working as a manager of a Digital Forensics Unit (DFU) with 0-5 years' experience conveyed:

> "The issue for me is the adverse effect of having to 'further' educate graduates in the day to day skills and attributes required in law enforcement around digital forensics. It can take 1-2 years for a graduate to be effective, which also represents a resource drain on existing staff. More field experience would be very beneficial, but extremely hard to come by. Some form of apprenticeship/work experience would be beneficial. Technical validation of hardware/software is also an area where new recruits lack knowledge or experience – something that is part and parcel of our day in complying with ISO17025 requirements."

This professional demonstrates the broad scope and experience a digital forensics practitioner requires, from standards through to legislation, from theory to practice to the applied practical experience which seeks greater knowledge and understanding. The professional also acknowledges, that for students and graduates, it can be difficult to obtain work-based learning within the discipline. They similarly express the opinion that "the bridge between industry and education is still too wide." Noting that "there are areas for research and development that [people] would be keen to work with education establishments on, but the bureaucracy and limitations make the benefits difficult to achieve."

This issue is recognised by many of the participants in this study, not solely professionals and is at the forefront of some challenges seen. Another participant notes a similar point, extending to the challenges of security checks which also make collaboration longwinded and difficult in some cases to implement.

Considering the challenges toward motivating industry and educational collaboration, these often impose problems with graduates and their lack of industry insight or replicable pressures of real-life experiences (e.g. backlogs, customer/business satisfaction, specific content and crime). With the observation that many respondents are employed in the public sector (e.g. law enforcement/policing), a question raised aligns to whether the difficulties in obtaining work-based learning are heightened due to costs associated with high security-risk roles, personal background security checks, further impact on workload and more. This is replicated by other participants who describe the situation where there are just "too many hoops to go through with security clearances …" that such collaborations can often be costly on potential industry partners where there is the growing necessity for compliance and efficiency.

Lallie and Day (2012) describe their view of these issues, exploring the relationship among universities and industry, highlighting that opportunities are possible but “it is after all a ‘matter of trust’” and, that engagement with industry does not stop at placement opportunities. Furthermore, while not a representative study of all students and disciplines, Tymon (2013) points out that “although experience is highly attractive to employers there seems to be an increasing reluctance for them to supply development in transferable skills” due to economic pressures. With cuts to public service funding, this stress becomes ever more prevalent in jobs sought within areas of policing such as digital forensics. Overall policing in England and Wales has generally seen a decline in the number of police officers (14%) and staff (23%) respectively between 2009 and 2016 (Disney and Simpson, 2017).

Further observations are made that student expectations are often, at the outset, centred towards the highest paying job or obtaining a job within the policing sector. One professional deliberates this point expressing the need for a “greater focus on commercial acumen as well as more conventional public sector/police [is] needed” where, they note that, “not all job opportunities are police work”. This has also been highlighted in this study by the academics themselves, pin-pointing the necessity to tackle student perceptions and expectations where job achievement and establishment of a placement are one of the first areas to address.

Further to this, issues highlighted were often centric towards keeping pace with technology, crime, and the requirements as well as pressures placed on industry professionals. One professional goes further to express there are “not enough graduates in the market, and not enough seasoned graduates with hands on skills working under pressure of a live client engagement”. Another respondent echoed this point continuing to identify they “would hire an experienced practitioner with no formal skills but live experience, over a well-qualified but untested graduate.” Again, focusing on the difficulties in obtaining practical experience within industry and the challenges educators face in providing similar pressures to real-life scenarios.

One interviewee raises the challenges of providing real-life scenarios where the discussion led toward noting “it can be tricky … one of the difficulties of getting up-to-date and interesting case studies is the fact that a lot of it has yet to come up to trial. Even if the police are prepared to let you go in and observe, you still cannot use it. You are always going to have a sort of delay.” Another aspect this interviewee discusses is the “pressure on the police[, where] they might consider they do not have the time to [help with these issues within the academic discipline]”. Contrary to this one professional with 6-10 years’ experience states “some educations are too far away from the real-life difficulties faced in digital forensics today. It seems like some educations have to create difficulties and scenarios of their own, and that these are close to non-relevant when it comes to practical work.” While this is one respondent, it is true that educators have to develop their own scenarios to educate potential new workforces. With the pressures and inability to use current real-life scenarios this again puts educators at a disadvantage and arguably one step behind.

With a number of questionnaire respondents mentioning issues where graduates have a "lack of real-world, hands-on experience", several suggestions for improvement were made supporting the need for greater collaboration between education and industry. For example:

- gaining experience through "perhaps more work placements" where interests are demonstrated outside the policing sector;
- several guest lectures with questions and answers; and
- the need for "graduates … to be realistic on gaining work experience and working with people[, noting] the best highflyer is of limited use if they cannot work to someone else's process – your work will not be recognised as valid if you don't follow procedures (often imposed by third parties)."

Some courses across HEIs in the United Kingdom offer placement opportunities as a year in industry or long modules as noted previously, this has been in response to the demand for practitioners with substantial experience. However, there are still several challenges in procuring placements within the discipline. Thus, they are not always embraced by prospective or current students and, to some extent, industry. Accounts from Lallie and Day (2012) highlight the need for students to be realistic in obtaining placements and how their focus must target a much wider domain than the one they seek to work. The authors recognise that there were often, at one institution, "[n]o students … placed within the information security/digital forensics domains" and there was a greater need to explore the wider computing sector as a source for placement opportunities.

Other authors such as Tymon (2013) highlight that the value of a placement to a student is not always recognised until their final year studies or on graduating. Where, the value can also be diminished by a sense of fear and anxiety (The Higher Education Academy, 2014). Several studies (Kyriacou and Stephens, 1999; Chui, 2009; Luhanga, Larocque and MacEwan, 2014) in the disciplines of education and healthcare demonstrate anxieties placement students can face such as, the feeling of incompetence, the fear of being dependent on someone else and someone unfamiliar, the fear of being judged along with the fear of not being accepted or being undervalued. Further, there are often hesitations due to balancing a placement with studies and work.

This issue has been observed at Canterbury Christ Church University, where the delivery of a placement module for the Computer Forensics and Security students has been added in the course's most recent programme review. The module requires students to have achieved a specific grade before they are able to consider taking this module; this to ensure that the student is able to cope with the pressures of holding down work experience alongside the continuous demands of their studies. Although most students each year can take this module, the take up has been low. The department has collaborations with many local businesses and public sector departments in digital forensics, however, curiosity lies among why cohorts over the past two years have shown reluctance toward placement opportunities. It may be considered that burdens placed on students (e.g. cost of tuition and living) as well as concerns for their studies and anxieties may be present in finding and keeping placements alongside existing jobs and study.

It should be recognised, there are many positives which counterbalance the anxiety of placements; such as, gaining direction for future careers, developing social and professional networks and increased opportunities for employment. A need for balance is required for different types of learner where, for some (e.g. surface learners), they are motivated by demands, fears and pressures. Yet, others will find these anxieties hard to work with. There is also the potential for gaps in expectations between all stakeholders (e.g., the student, the university and the business); students are taken outside their safe zone and can feel concerned with considerable responsibilities and accountabilities they now hold.

Anecdotal evidence by academics and graduates within this study demonstrates that numerous students have been able to obtain a placement, volunteering role or working within law enforcement directly after graduating across several institutions. This may indicate that there is a common understanding and awareness among some educators and employers towards the potential employees; i.e., graduates showing their ability to learn and drive within the discipline. Again, though very much residing back with the attitude of the individuals and their soft-skills in integrating with a team as well, the ability to learn and develop quickly.

7.3.1.4 Experience versus education and training: the views of professionals

With experience anticipated as a likely dimension, prior to delivery of the questionnaire, a separate question was used to recognise whether experience, for the professionals, is more important than qualifications and training. Used as a source of reflection toward the end of the questionnaire, participants were asked the freeform question “Do you believe experience is more important than qualifications and training?”. It might seem counter-intuitive at this stage for the use of a freeform answer, why would one not use a multiple-choice question.? However, this question looked at exploring any explanations to provide more meaningful results.

Twelve professionals felt both were equally important. Some noting "experience is worth more", "basic training is no use without some experience" and that "an individual with limited experience … might be very proficient very quickly and can offer other soft skills". This is different to the opinion expressed by a participant previously who felt issues relating to graduates around the length of time and resources it takes for a graduate to be effective due to further education and experience of the daily skills.

A further eleven felt that, yes, experience is more important. Four professionals stated no, with three stating it depends on factors such as "the level of job and qualifications", "on the type of experience", and "on the role and issue in hand[, where] some areas lack recognition and training and still need to [be] explore[d]".

Respondent years' experience	Yes	No	Both	Depends
0-5 years	4	1	7	2
6-10 years	5	2	2	0
11-15 years	2	1	2	0
16-20 years	0	0	1	0
21-25 years	0	0	0	1

Table 7.3 – Questionnaire Responses: Relationship between Years' Experience and View of Experience

Looking at responses in greater depth a correlation exists between years' experience and view on the worth of experience. Table 7.3 illustrates how most individuals with 0-5 years' experience felt a healthy balance were required ('Both'). Yet, those with slightly more experience (e.g. 6-10 years') felt experience was more important.

The potential bias of these individuals should be noted at this stage. All respondents are professionals with several years' experience, so by now they would have reaped several benefits through experience, particularly in areas of investigation and so on which could influence their views on the importance of experience over education and training. Although, some respondents show understanding that "with time comes experience" and that there "is a reliance on having qualifications to get yourself noticed in this field".

7.3.1.5 Practical experience and hands-on curriculum and learning

Another debate highlighted by questionnaire responses coincides with the need for practical experience: the use of vendor specific tools. There are some obscurities in the responses where, one respondent notes that graduates have "limited hands on experience using tools", yet it is said by another that "University courses can often use forensic programs that do a lot of the hard work for you using scripts … without giving much of a background unless you went on a [vendor]-issued training course".

Vendor tools are utilised within both disciplines to help professionals conduct examinations. It is clear that although vendor tools must be taught and utilised on a higher education course, the consensus of many professionals is that the tools should complement a graduates' knowledge, skills and abilities. As one describes, a "vendor neutral approach means a wider range of forensic methods are shown." At Canterbury Christ Church University (CCCU), a Forensic Computing course has been running for ten years, under a number of incarnations, where in most recent years feedback received from an employer of some graduates recognised how students are provided with a solid foundation of theory yet provided with an insight into how to use a number of vendor specific tools, albeit they still require the necessary vendor-specific training. This was reiterated by graduates in chapter 6 who noted that although they were not given a massive amount of content on how to use tools, the "lower-level tools" as described by one academic in chapter 6 and the thorough theoretical content they were provided with gave the graduates a breadth and depth of knowledge to apply as technology and crimes advance.

At CCCU it is believed a balance of theory and practice is best and, to some extent, established using a placement module, problem-based learning, case studies and guest speakers. While the course lecturers are able to recognise and highlight difficulties with resourcing and industry inclusivity. Several professionals express the issue of some courses and graduates being "good in theory but the skills and tools are redundant", or "theoretical skills and good grades, but unable to use these in practice". Again, concentrating on the need to rely less on the tools and a requirement for courses to "provide good theory". What these professionals are expressing is the necessity for courses to avoid sole reliance on utilisation of vendor specific tools due to the downfall associated in not providing a well-rounded graduate.

One computer forensics investigator with 6-10 years' experience felt

> "[s]ome educations are too far away from the real-life difficulties faced in digital forensics today… [where,] the outcome of some courses are solutions to problems that doesn't exist, and the techniques used are not applicable in real life scenarios. [They expect] a graduate to know the basics of computer forensics, and to understand how the different forensic tools work, rather than to know which buttons to press but being unable to explain what the application does. [They] also expect a graduate to be able to work his/her own way around unknown obstacles that might arise; e.g. how to start working on an unknown file format, document unknown database files, find out how an unknown app works and so on."

These professionals note, it is not just the skill of being able to use a tool which does much of the work for you, as noted by James and Gladyshev (2013a) as "push-button forensics", it is the necessity for soft skills (e.g., reporting capabilities, networking and the ability to explain oneself in layman terms), and further a vast range of technical capabilities from data extraction and analysis (e.g., the individuals ability to capture and extract data without vendor tools) of an abundance of data sources (e.g. computers to mobiles and tablets, networks to security, emerging technologies and so on).

With a sweeping range of skills, experiences, disciplines and topics to cover courses can (particularly in training scenarios) seem short and are often restricted by their own resourcing problems and requirements, similarly to their industry counterparts. Looking to a participant in the education sector, they discussed how “HEIs cannot give all the knowledge, experience and expertise required by the industry within a three-year course”. Noting, course providers “may not have human resources with adequate industrial/professional exposure in their teaching teams”. Digital forensics as a discipline has previously been observed to commonly lack the resources required causing it to be a major challenge (chapter 2 and chapter 5); in educational practice, this is possible cause for courses to potentially lose focus on the discipline or topics of interest, even to the extent of providing little vendor neutrality.

For instance, one respondent noted they have found there to be “not enough focus on computer forensics and more based around programming etc. (general computer skills which are not particularly relevant to the role)”. Looking deeper into this, of course the fundamentals of computing are key to a digital/cyber professional, however, the point this professional is seemingly making is that of, for instance, the need for extensive programming knowledge and the general Information Technology skills (e.g., user-based support, word-processing skills). Although, it can be argued that, programming and scripting skills are at the forefront for a cyber security practitioner and are becoming extremely sought after, in comparison to before, for a digital forensic practitioner. These programming and scripting skills are more sought in the discipline for several reasons, for example: the need to extend the functionality of tools, develop own tools and to conduct automatic processing. A similar point raised by graduates in chapter 6.

One professional, with an experience of higher education, expressed their course was good, with another voicing their degree was of great use, particularly for “gaining a wider knowledge and understanding of the theory”, however, that in terms of “practical element[s these] could be expanded”. Another respondent expressed their view on the inexperience of presenting and giving evidence in court. They note how in an educational context relay of information can be unrealistic as “It is easy to talk technical with other technical people . . . but interaction with those who aren’t technical can show” how talking and presenting in layperson terms is difficult and “can show misunderstandings”. They indicate that lessons on presenting evidence in a court room and relaying information would be useful. In some courses, this is achieved through court room-based scenarios with cross-disciplinary departments (Kessler, Simpson and Fry, 2009; Crellin, Adda and Duke-Williams, 2010; Irons and Thomas, 2016). These are scenarios where students are provided with the chance to extract data, analyse the contents of the devices and report their findings, presenting them in a court-like scenario, including judge, barrister and jury. However fun this practical may be, it is a time consuming and often difficult scenario to apply requiring an abundance of, and central, management. At CCCU there have been numerous discussions among law and computing staff to set up a scenario that facilitates this form of learning for both sets of students, however, such complexities have limited this set-up. In turn setting this up has turned to Bond Solon, a legal and information training company providing expert witness cross-examinations (Bond Solon, 2019). Again, addressing issues educators face when resourcing, planning and implementing a highly multi-disciplinary subject.

Overview provided by these above-mentioned questionnaire participants provides insight into the thoughts of just a few professionals after graduating and, having gained some experience on-the-job. These views demonstrate that courses can provide students with the fundamentals for which they can continue to develop and master with greater experience. Although, a greater number of practical elements could be included in degree programmes, it should be said that several authors have documented the use of scenario or problem-based learning and case-based learning as techniques which allow for greater learner centric approaches and engagement, practical and enquiry-based learning and development. Arguably, skills which should be second nature for an effective digital forensics and/or cyber practitioner required in all walks of their role.

7.3.2 The view of professionals: expectations of graduates with a digital forensics/cyber security degree

With 62 percent of questionnaire respondents articulating some input when hiring new employees (combining ‘yes’ and ‘sometimes’ response numbers), it was beneficial to identify expectations of graduates from the professionals’ perspective. Questionnaire participants highlighted several subjects and areas where they felt graduates lack, or there is a skills-shortage. In the words of one online respondent, there are “too many [topics, specialist areas and skills] to list”. This supports alumni views that any student or graduate in the discipline should be prepared they will not know everything and the career they pursue requires motivation for continual learning and development. Following on from this response the individual listed several expectations they would have at a fundamental level:

> “Common architectures of PC, servers & virtual servers; Navigating/manipulating files on DOS and Linux command lines; Imaging techniques (GUI tools, command line, dedicated hardware, Apple devices, mobile phones, Volatile memory, etc); Network technologies, e.g., Ethernet, Wi-Fi, Bluetooth, etc.”

Analysing this result further identifies the need for what they highlight to be fundamental computing knowledge and skills and basic forensic competences such as, imaging, system workings and tools which can be used in a forensic manner to extract a range of data.

Another respondent summed up their view stating:

> "Python scripting is a plus, as is EnScripting if they were to go down a more vendor-specific route, but a good understanding of ACPO principles and how deleted data can be recovered, and why it is recoverable, is the type of knowledge you'd expect to know. Knowledge of computer components and different types of devices is a big plus, as not every device we get is a computer (mobiles/USBs/routers/sat navs/anything that can store digital data!)"

Again, a big focus on the fundamental components, devices and data. One professional in the questionnaire voiced a similar opinion to those of interviewees, that graduates with a degree in digital forensics should hold knowledge and skills "the same as a comp sci degree but with additional forensic modules". However, academics have noted how they feel a digital forensic degree should not be based around such a definition, feeling that digital/computer forensics courses are not computing/computer science with added modules. This conflicting view represents again, the disparity while defining the discipline. Furthermore, one graduate felt they may have taken a different path into computing (e.g., programmer or developer) had they pursued a degree in computing or computer science opposed to digital forensics. Professional interviewee and questionnaire respondents, however, did note topics intrinsic of both computer science and digital forensic/cyber security courses.

This left the most highly noted expectations as basic/fundamental computing knowledge and skills, networking principles and fundamental understanding and competencies in forensic analysis. Operating systems and file systems were noted on thirteen occasions; again fundamentals of computing. Handling of data, data recovery and analysis were mentioned a total of ten times with an extra four instances for imaging technologies or of devices. Scripting/programing was another topic which was mentioned on five instances with a further two occasions for DOS or command line instructions or file manipulations. Linux was mentioned on six occasions ranging from systems to as an investigative tool.

Chapter 2 of this study highlighted the omission of mobile forensics within course module naming conventions; mobile forensics was raised by questionnaire and interviewes. Several individuals noted how devices are no longer just computers and that graduates should have experience and knowledge of mobile and cloud technologies. One epitomises this saying improvements for HE would include "possibly more in depth about mobile phone forensics as this is a developing market. Other types of forensics like databases and cloud."

Mobile technologies were, in particular, mentioned by a professional with 0-5 years experience and whose specialist area was Sandbox Analysis Tools. The individual's responses were quite strong and took a negative direction firstly by stating, "you're not teaching SEIMS systems!!!". They commented that to improve higher education by "includ[ing] SEIMs; remain[ing] with EnCase [but] drop[ing] X-Ways as [they state it is] useless in Corp IR". Further when asked about skills shortages among graduates looking for employment, they continued to state they had found the graduates to have "Zero knowledge of SEIMs and Cloud technologies". Interestingly, the professional noted having no input when employing people nor any related educational experience and few years' experience (0-5) in the discipline. Arguably their opinion is influenced by their own experiences and viewpoint that experience is more important than qualifications and training.

Furthermore, the respondent voiced their opinion and feeling that "the BCS[, the Chartered Instiute for IT] makes universities set work based upon a set framework of useless skills such as, Databases". Stating how it "is not ideal in the workforce" nor for securing a role based on their own experience in threat detection and prevetion. They also state that "the emphasis on mathemeatics is null and void in the workplace". The respondents claim that mathematics is not at the forefront for practitioners within the discipline, may be supported by the omission of this as a knoweldge or skillset among questionnaire responses and courses described in course analysis.

This point is also interesting as academics and graduates alike reflected how database knowledge within digital forensics is a key component, with some CCCU graduates noting how specifically database forensics would have been beneficial in their curriculum. Databases were also mentioned by two other respondents as expecations of a graduate/professional and research in the domain has stressed the importance of database forensics for capturing data stored in, for example, applications and systems (Beebe, 2009; Olivier, 2009; Garfinkel, 2010). Meanwhile, most recent course standards discussed in chapter 3 (Joint Task Force on Cybersecurity Education, 2017; NCSC, 2017b; Newhouse *et al.*, 2017) do not highlight databases as a specific area of interest for defined digital forensic roles or courses, however, they do identify with analysis of digital evidence from and including various data types and sources.

In addition, investigative skills and techniques were found on four occassions throughout the online questionnaire, however this can also be inferred in instances of chain of custody, forensic processes and procedcures and all topics such as, analysis, recovery, handling of data, imaging and more. Investigative skills are fundamental to the success of an investigation, however, these skills are, for the most part, excelled when practically applied, learned and developed on-the-job. Educational programmes can however, provide skills in investigations through problem-solving and scenario-driven appraoches to learning and assessment. In-depth analysis identified (Figure 7.2) six key areas professionals questioned online felt are, and should be, expected or required of graduates with digital forensics/cyber security related degrees. However, softer skills such as presentation, management and client handling are discussed later in section 7.3.2.4.

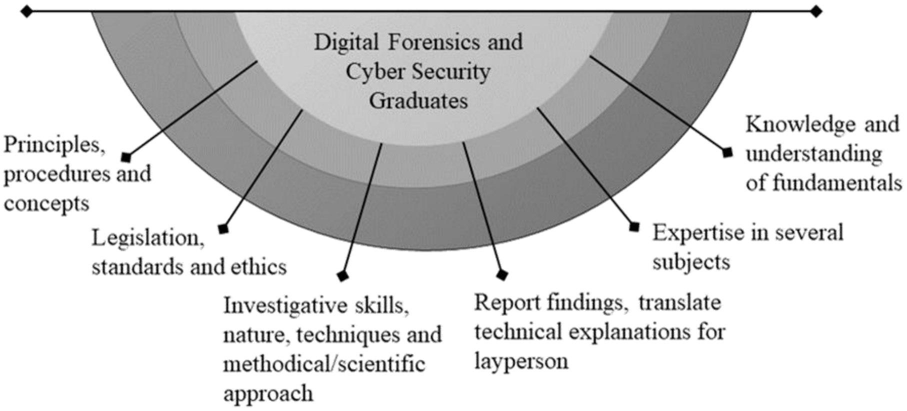

Digital Forensics and Cyber Security Graduates
Principles, procedures and concepts
Legislation, standards and ethics
Investigative skills, nature, techniques and methodical/scientific approach
Report findings, translate technical explanations for layperson
Expertise in several subjects
Knowledge and understanding of fundamentals

Figure 7.2 – The Skills Model for Digital Forensics and Cyber Security Graduates

Throughout this thesis and both professional interviews and questionnaire responses, there have been specific themes or trends which can be ascertained as key points of this research and include, but are not limited to, experience, legislation and ethics, mobile forensic analysis, programming and soft-skills. These are discussed from a professional perspective in the following sections.

7.3.2.1 Legislation, Ethics, Compliance and ISO 17025

Looking more closely at the responses, professionals felt graduates should be expected to possess good knowledge and understanding of a range of principles, technical and non-technical procedures and a range of legislative, ethical and compliance materials. For instance, one questionnaire participant states that “a good understanding of ACPO principles and how deleted data can be recovered, and why it is recoverable, is the type of knowledge you would expect to know.” Moreover, another respondent adds they would expect a graduate to have covered “the qualities of forensic processes and that we are experts of facts”. This is something which academics, graduates and students alike in chapter 6 felt were important aspects of learning.

Furthermore, two respondents with between 6 and 15 years’ experience expressed the awareness of International Organization for Standardization (ISO) quality standards as important. Reference is aimed at the “knowledge of forensic principles requirements of ISO 17025” believed by one respondent to be something which they would expect graduates to have covered at degree level. Respondents in the questionnaire also noted the inclusion of such standards (e.g. “ISO accreditation insight”) when asked what they would include or do differently in higher education courses. This may suggest that courses omit teachings relating to these standards, at least courses which professionals have experienced or know of. Another respondent highlighted that “technical validation of hardware/software is an area where new recruits lack knowledge or experience - something that is part and parcel of [every] day in complying with ISO17025 requirements”. This study recognises that the professional works closely in delivering compliance with ISO standards/accreditation within their workplace introducing an element of bias; however, with a handful of responses mentioning ISO standards and little evidence of course content and clarity during analysis in chapter 2, this thesis argues ISO standards such as ISO 17025 must be included within the curriculum.

ISO standards are internationally recognised specifications for services and systems used to ensure quality and efficiency (International Organization for Standardization, no date). In most recent times digital forensics laboratories have been susceptible to the ISO 17025 standard which as of October 2017 was mandatory for digital forensics labs within the UK impacting how examinations are conducted looking at the competence of laboratories (International Organization for Standardization (ISO), 2017). Previously the specification was used to standardise the forensic laboratories of testing and calibration in relation to DNA, fingerprints, a wet forensic approach. Due to the current omission of standardised laboratories and practices within digital forensics, the standard is now used to encompass digital labs to show standardisation within the discipline for laboratory and tool compliance. Compliance with such a standard within the digital environment for some is controversial (Beardmore, Fellows and Sommer, 2017, pp. 38–45). Many commenting that this accreditation is not the solution to the problem and position of digital forensic standards. Some have noted how they are “onboard with ISO compliance” but note it provides several challenges for them within a technically advancing discipline where workstations require a mass of, and revision of, forensic software due to the need for re-verification (Beardmore, Fellows and Sommer, 2017, p. 41). Some believe that instead “a standard to cover the testing of tools should be implemented and vendors”, where responsibility lies with the vendors (Beardmore, Fellows and Sommer, 2017, p. 42); again, addressing the open versus closed source debate (Moore, 2006) and the cause for change in digital forensic software vendor responsibilities.

One comment on a forum discussing the push towards the ISO standard in digital forensics states that the problem is not working toward or complying with such a standard, it is the unsuitability and costs of the applied standard which is described as more akin to wet-based forensics:

> “almost every single forensic analyst working in the UK today strongly supports the idea of having a standard, it's simply the fact that 17025 is an inappropriate standard for this particular discipline.”
>
> —(The Court Jester, 2017)

With this in mind, Beardmore, Fellows and Sommer (2017) found that less than 25 percent of 176 professional respondents felt they had a good or high understanding of the standard. Further the survey found that 25 percent of respondents openly expressed they had a poor understanding of ISO 17025.

Keeping this in mind and focusing on comments from respondents in this study; if the very professionals who must comply with these standards in their everyday roles meet troubles, lack of awareness and/or training, can it be expected that students or graduates have a good understanding of these specifications? Therefore, the degree to which these standards should be covered is yet to be deliberated and there are still causes for concern surrounding the suitability of such standards within a discipline which is dependent upon continuous technological growth (Horsman, 2019). At minimum, a course should cover brief understanding of compliance and the standard, as it affects digital investigations.

Though ISO 17025 is not the only standard which some may argue students need to be made aware of throughout their education. Respondents noted generically ‘ISO standards’ to be important; where, other relevant standards are a requirement of a forensics practitioner. Some include those in the catalogue ISO/IEC SC 27 (ISO, 1989) namely IT Security techniques. The catalogue contains 184 separate standards which cover a range of aspects in relation to addressing security, privacy and digital evidence (ISO, no date). Several standards which pertain to digital evidence include ISO 27037; ISO 27041; ISO 27042; ISO 27043; and 27050, to name but a few.

Examples which demonstrate the need for, at minimum, student awareness of these standards are evidenced by the contents of these standards. ISO 27037 was published in 2012 and confirmed (i.e. remains current) in 2018 (ISO, 2012a) and concerns the guidance of the preservation of digital data which may be of evidential value covering fundamentals such as, identification, collection, acquisition and preservation of digital evidence. ISO 27042 covers Information Technology Security Techniques, providing guidelines for digital evidence analysis and interpretation (ISO, 2015a), whereas ISO 27043 provides guidance on incident investigation processes with the involvement of digital evidence (International Organization for Standardization, 2015b). More recently, although not explicitly mentioned by participants of this study, two parts of an international standards catalogue ISO/TC 272: ISO 21043 relating to Forensic Science have been published with three further parts (at the time of writing) under development (ISO, 2012b). In a House of Lords Select Committee exploration into Forensic Science, The British Standards Institution (BSI) noted these standards "will be applicable for digital forensics" (Select Committee on Science and Technology, 2018).

Other understandings of several legislative material such as, the Regulation of Investigatory Powers Act (RIPA), Police and Criminal Evidence Act (PACE), Criminal Justice Act (CJA), Computer Misuse Act (CMA), Data Protection Act (DPA), General Data Protection Regulation (GDPR) and others are vital to a daily job in the role of a digital forensics professional. Further to this, techniques and methods applied to imaging, finding, extracting and analysing data and the underpinnings of digital devices, their innerworkings (e.g., operating systems, file systems) and networking/infrastructure are exhaustively mentioned by participants. These findings demonstrate the importance of standards and legislation for practitioners within digital forensics. It may be argued that participants of this study who mentioned regulatory and legal components are from public sector roles such as, police environments as opposed to corporate counterparts which involve more client liaison. However, legal and regulatory knowhow/acumen is still a requirement for each practitioner. Some academics have argued that while there is a distinct lack of modules (chapter 2 – course analysis) relating to legal and regulatory issues, these are issues and teachings which for most are included throughout the curricula and support both corporate and public sector investigative roles.

7.3.2.2 Understanding and Experience of Industry Tools

Respondents also discuss the range of tools used within both digital forensics and cyber security to help conduct investigations. Some address expectations or issues directed toward graduates' experience, or lack of experience and understanding of fundamental tools used within the discipline. One questionnaire respondent with 0-5 years' experience having completed a related degree acknowledges part of this problem is down to the "limited hands on experience using tools" within education.

> "Good understanding of the current threat landscape and techniques and tools available to handle them. Knowing limitations in tools is very important."

One professional interviewed stated that they would at a minimum "expect students off their own back, whether their lecturers have told them to or not, to explore the free tools and see how they work". Commenting that "a good understanding of how imaging tools work as well as the free and open source tools" is not overestimated at a graduate level. They continue to note that "it would be a bit harsh to say [graduates] should have a full understanding of all the major industry used tools because they are different kettles of fish." These are something which all interviewees have commented are delivered by training and at education a minimum understanding of how the tools are used and how they work at a basic level are appropriate. This was something which CCCU gradates noted was an issue for them when they entered and applied for jobs, as they felt they had little experience with the well-known tools. A positive for CCCU graduates was their awareness and use of open source tools and understanding of fundamentals.

Again, prominent topics include network analysis and understanding of network technologies, knowledge of operating systems e.g. how multiple operating systems work (Windows, Linux, Mac and mobile technologies), an awareness and ability to perform data acquisition techniques, programming/scripting capabilities (particularly, with the ability to use command line and Linux), and penetration testing/ethical hacking. Other key topics such as general computing fundamentals and knowledge of common architectures, investigative skills, principles and procedures, and chain of custody were noted.

Some participants identified how they felt relevant skills-shortages and practical education and training covering technical specialisations were required in, for example, encryption/decryption. One participant mentioned how they felt that an issue with current education and/or graduates were their lack of "practical experience with decryption using current forensic tools". Looking to the curricula, encryption and decryption are mentioned in current frameworks relating to cyber security, where coverage includes the need to know basic and advanced cryptographic concepts (e.g., ciphers and algorithms, integrity and confidentiality and authentication) (Joint Task Force on Cybersecurity Education, 2017, p. 24). However, examining these documents by categorisation of digital forensics and omitting cyber security, these documents do not highlight such as a focus. For digital forensics curricula programmes on offer, many consider cyber security and digital forensics on the same course (as discussed in chapter 2 – mentioned across 11 courses/module titles), and now prescribed by new frameworks (Joint Task Force on Cybersecurity Education, 2017; NCSC, 2017b; Newhouse *et al.*, 2017). Highlighting the lack of reference for these specific topics in such courses and in current frameworks, supports these professional views for more coverage required of cryptographic concepts and applicability of current forensic toolsets. Documentations, however, consider the use of and, in some instances, the limitations of tools in digital forensics to extract data using all-in-one suites and data carving techniques. Other specialist areas mentioned by respondents included cloud forensics, the dark web, app development and online investigations (e.g. open source intelligence/OSINT), databases/SQL, and emergent technologies.

Professionals were asked if they felt frameworks and certifications have any impact on education and graduate employability, mixed views can be found (Figure 7.3).

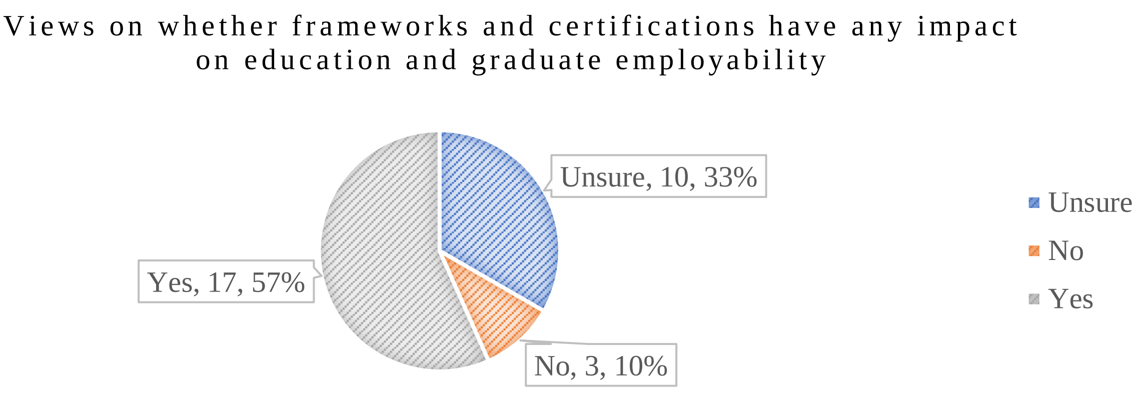


Figure 7.3 – Professional views on frameworks and certifications on education and employability

7.3.2.3 The programming debate

Previously, chapter 6 has highlighted how the researcher has experienced students and applicants who are looking for a course which contains little programming; yet, graduates and academic responses have highlighted how as a digital forensic practitioner, you cannot shy away from programming/scripting. This debate continues with the views expressed by professionals in this study.

Yet other responses highlight how courses may be focusing too much on computer science with a flavour of digital forensics with not enough depth. For example, an investigator responding in the questionnaire who holds 6 -10 years' experience specifically focusing on computer and mobile examinations expressed how they feel there are issues with current HE and graduates in that courses offered often do "not provide enough focus on computer forensics and are more based around programming etc (general computer skills which are not particularly relevant to the role)". While the respondent expresses programming skills are not "particularly relevant to the role", this does depend on the job they undertake. Graduates in chapter 6 noted that while the main portion of their jobs are push-button forensics, they need to be, from time to time, able to create a script that manually completes tasks to corroborate or extend tool functionality.

Additionally, a respondent who works as a Data Forensics Investigator and completed a Computer Science degree highlights, they were offered a singular module on their course which focused on forensics. Which again, reflects only a short period of time and credits at degree level to cover a multitude of digital forensic subjects. The likelihood with many courses structured like this would often show the student has received extensive coverage of multiple modules a forensics or security student would receive such as databases and operating systems but with more focus on programming. Looking back at the professional with a Computer Science degree, they recall that,

> "The module did cover a lot of forensics and offered to do the ACE exam ... [and] had EnCase but only version 4 due to pricing. They taught about the Computer Misuse Act. However, speaking to a friend … who did Forensics at University I have heard that sometimes they don't do as much forensics as is offered for example they didn't use EnCase and didn't go into much forensics about MFT, unallocated etc."

The participant finds that they would opt for courses to go "more in depth about mobile phone forensics as this is a developing market. Other types of forensics like databases and cloud. Possibly some law subjects (Not just the Data Protection Act)". Supporting responses provided by graduates and acknowledgements academics have made based on insight from professionals.

7.3.2.4 The importance of soft skills

For a digital forensics or cyber security professional, to achieve competency and to become an effective practitioner, interviewees and questionnaire participants noted the importance of soft-skills as well as technical skills/knowledge mentioned by academics in chapter 6 and through the literature (Whitten, 2008; Pérez *et al.*, 2011; Floyd and Yerby, 2014; Govan, 2016). Professionals were asked, freeform, to express how important soft skills were within such professions. Coding responses found soft skills to be highly important across all roles. Of the 30 professionals just 3 professionals expressed mediocre responses (e.g. moderate, somewhat important and useful) where all others felt they were "quite important" through to "very important" and "mission critical". Several professionals, as identified previously in this chapter, note these skills to be very important in ensuring one can, for instance, communicate findings for varying technical abilities. Although, communicative skills (e.g. interacting, articulation/conveying information) were a high priority among the skills noted by professionals, Figure 7.4 also demonstrates further soft-skills expected of a graduate, ranging from problem solving abilities, attention to detail through to report writing skills and management skills (e.g. project, time and client side). Though, this is not an exhaustive list of all soft-skills required for an effective practitioner or graduating individual, but several which are paramount to a graduate's abilities.

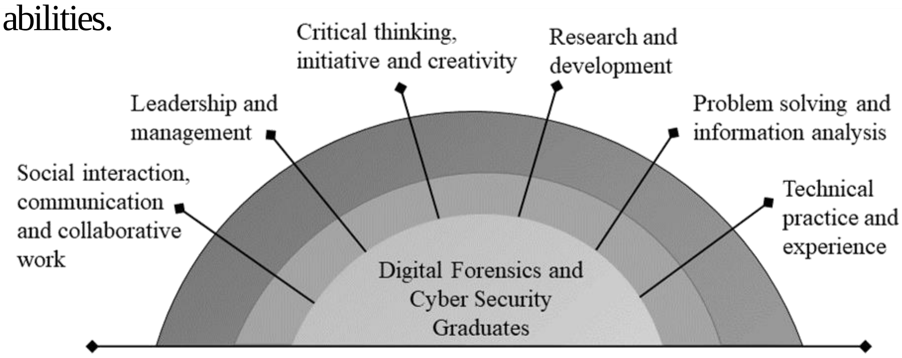

Critical thinking, initiative and creativity
Research and development
Leadership and management
Problem solving and information analysis
Social interaction, communication and collaborative work
Technical practice and experience
Digital Forensics and Cyber Security Graduates

Figure 7.4 – The Skills Model for Digital Forensics and Cyber Security Graduates

A common theme which recurred was the lack of practical experience and people skills, with one professional summing up their view with “great tech skills seem to correlate with terrible people skills”. Professionals want to be sure that an individual can communicate effectively and be able to explain the what’s and why’s relating to digital evidence based on the facts found.

For clarity, further understanding of known skills shortages or inexperience observed when employing graduates was sought. Professionals mentioned issues such as a lack of, “basic technical skills (e.g., ability to read/manipulate hexadecimal, working with offsets and tables), basic coding skills and reverse engineering, familiarity with industry standard tools and inabilities to troubleshoot from first principles”, basic knowledge of technical security or information technology. This is interesting as academics in this study discussed how their courses are used to ensure students, and in turn graduates, have the knowledge and understanding and technical competencies to carry out the most rudimental tasks of a digital forensic practitioner. Similarly, graduates from CCCU highlighted how manual carving, use of Linux and open source tools along with the fundamental learning of operating systems, networks and databases was essential and dominant to their success in gaining employment. This may once again shed light on the diverse coverage of course quality across the UK or the troubles students/graduates maintain in their awareness and ability to contextualise their learning with practical and on-the-job tasks.

7.3.3 The view of professionals: issues with, and suggestions for, current digital forensics/cyber security training programmes

Again, questionnaire respondents were open about issues they had experienced with digital forensics and/or cyber security training programs, providing suggestions for improvement. Mixed views were expressed ranging from “poor and almost just an advert for a product” to “positive” and “informative”. For the most part, coding showed professionals felt training is different to education, in that, training courses are largely fit for purpose and product centric teaching candidates how to perform tasks (i.e. short-term learning).

One professional epitomises these experiences stating, training courses “vary from too simplistic to too vendor/tool specific [with] not enough [to] cater for getting the best results regardless of tools or experience.” Where, another communicated they “would tend to lean away from vendor specific training”. Similarities can be made here with previously mentioned fears towards too much reliance on vendor specific tools in higher education.

Commercial based training, for some, “are mainly focused on teaching how the[] applications work”. With several respondents noting such courses are often limited, lack the fundamentals and lack deeper explanations. One respondent finding that, in some cases, instructors know very little. In the words of the computer forensics investigator previously quoted:

> "you need the basic set of skills before you can start using these applications in real cases. It's important for the investigator to understand what the tools are trying to achieve, instead of using applications uncritically. Most applications can either be used in a wrong manner or contain errors, and it is of great importance that the investigators are able to discover erroneous output."

With the "focus often on tools and automated analysis" comes the question for improvements to training courses to ensure practitioners do not become completely driven and reliant on the tools they learn to utilise. Again, pinpointing the notion that the practitioner must be able to understand the fundamentals, techniques and how the tools work. One respondent with 0-5 years' experience states that they would improve training by having "less Vendor specific, more basic forensics and grinding through the hex …", something which was mentioned by both professionals and academics alike.

Furthermore, a digital forensics practitioner in the court of law needs to fully understand and be able to explain all techniques of data collection, data analysis and so on, before they can call themselves an expert. What some participants note is the use of training in the need to demonstrate as a specialist or expert. Where, qualifications and certifications can help to demonstrate a practitioner's ability, relevance and reliability along with experience. Thus, articulating a sound understanding of concepts, theories, techniques and so on to be paramount to a practitioner's effectiveness. One respondent, with several years of experience, believes "an awareness of Linux, programming, Windows, HFS+ for example is good enough because you can always be trained to become a specialist later on through training and gaining experience." However, the fundamentals and techniques are far more important than the substitute reliance on tools.

Again, improvements suggested for training courses ranged from ensuring tools are up-to-date with course content and required content based on current technologies and crimes, more technically specialised courses, more time for courses, through to more interaction, scenario and problem based hands-on experience and more vendor neutral training. With these fast-paced multi-disciplinary subjects it is key that design of course content, as Rowe, Lunt and Ekstrom (2011, p. 118) explain, "is not exclusively connected to a specific technology or piece of software, but focuses on concepts, methodologies and skills that will endure the test of time".

One respondent, with 11-15 years' experience in policing working as a Digital Computer Forensic and Cybercrime Investigator noted that making training courses "more scenario based and integrat[ing] technical skills as a means of getting to answers" as crucial to the learning of such a practitioner. They continue to identify that a digital forensics and/or cyber security practitioner should be a problem solver, critical thinker and should not take anything at face value, asking questions and querying responses and potentially results. Stating; "Digital investigators should learn to ask the questions and not just give random answers like 'here are all the pictures'." Thus, thinking outside the box and having a questioning nature.

Costs were another improvement sought after, where it has been previously addressed in chapter 5 that courses can be expensive, particularly for individuals or sectors with limited support for funding. Results show that it is not only limited within the UK, with one professional expressing for their country the links between academia, training and industry are only on an international level meaning vast quantities of money are usually required to send professionals on courses where, again, there is often no money.

7.4 The view of professionals: overview of current skills-shortages

Based on the polled individuals in this chapter, several areas were identified as key issues in higher education and training. Furthermore, participants were able to highlight some areas/skills they believe where there are currently skills-shortages in the industry. Snippets of responses for this question shown in Table 7.4 demonstrate that there are still a vast range of skills which need to be developed, where higher education courses can look to include or focus on improvements such as, specific operating/file systems, malware analysis and incident response, live forensics and, again, more practical hands-on experience.

What are the skills-shortages within the current industry which higher education or training courses should tackle?
Certainly, how to configure systems to be secure (as by default they're not). Perhaps basic knowledge of how an ICT system works too so graduates have a more rounded knowledge?
How to deal with malware/ransomware attacks
Greater understanding of malware and network attacks/breaches. Conventional 'volume policing' has less focus at present
Teach students SEIMs, Cloud and IDA!!
Fuzzing
Prop for getting rid of useless certificates, develop contacts with the businesses during education. Not much you can do besides that, it's an industry problem with individuals trying to hire people that don't exist.
Malware and security review. Incident response.
Security architects
Growing Shortage of Security Skills; Defending - Firewall, IPS, WAFs, Layer 7 defences; Attacking - Kali Linux, Metasploit, Nessus
Blockchain; GDPR; Decryption
SIEM skills
Live forensics is a pressing need
Courtroom skills training.
Hands on work experience
Linux & Apple file/operating systems
We don't have any trouble recruiting so I'm not sure skills shortages are a problem. Retention however is a problem but that's due to pay.

Linux/Mac knowledge is lacking certainly, most people stick with Windows as that is what they know and have understood.
There is a shortage of people with mobile forensics skills
Talking
Skill shortages in mobile phones because they are turning more into computer devices.
All
Investigation skills
Practical based forensics. Much of what is covered is theory based and students come from university with very little idea as to how to actually do specific tasks.
Practical experience with common tools
The issue for me is the adverse effect of having to 'further' educate graduates in the day to day skills and attributes required in law enforcement around digital forensics. It can take 1-2 years for a graduate to be effective, which also represents a resource drain on existing staff. More field experience would be very beneficial, but extremely hard to come by. Some form of apprenticeship/work experience would be beneficial. Technical validation of hardware/software is also an area where new recruits lack knowledge or experience - something that is part and parcel of our day in complying with ISO17025 requirements
There should be more focus on the amount of data in cases, and how to find your path through all the unimportant stuff.
There is all kind of digital forensic courses needed in my country.
Assessment of treads. Presenting a plan of process to obtain the wanted result.

Table 7.4 – Professional Questionnaire Responses: Skills-shortages in the current industry

7.5 Summary

This chapter has highlighted topics which professionals felt were lacking in current graduates, skill-shortages and perceived improvements which could be implemented in educational and training scenarios. These are discussed further in chapter 9, where similar views among stakeholder are pulled together. Much of which has centred around the need for more coverage on topics such as, mobile forensic investigations, hands-on experience and the need for more scenario-based learning on training. A theme common among many expectations from professionals of graduates was undoubtedly a solid and fundamental understanding of computer components, systems and architectures, data recovery and analysis and networking at a more in-depth level (e.g., the ability to work with hexadecimal data and not just the forensic tools). Furthermore, expectations included softer skills in the ability to communicate, present evidence, keep an audit and chain of custody, people/general management skills, multi-tasking and pressure handling skills.

8. DIGITAL FORENSICS EDUCATION: A VIEW FROM THE PUBLIC

INTRODUCTION

So far, this study has shown the views of target groups with a direct involvement with digital forensics as well as cyber security. Highlighting the need for in-depth and fundamental understanding of the subject and of specific specialisms, through to industry and educational collaboration. Capturing the perception of members of the public adds insight into what is understood of digital forensics and/or cyber security by a wider audience. It also adds the possibility to understand what they feel needs to be tackled in society and what they believe law enforcement should focus on in relation to digital/cyber-related crimes. Interests were also placed on finding out views of individuals who have fallen victim of such crimes, the crimes committed and their response to these situations.

8.1 Recap on the Method

To capture and understand these general perceptions, a questionnaire was distributed across social media platforms, and via convenience through known individuals, with the intention to capture viewpoints of a fifth target audience: the public. Sampling methods and questionnaires as a method in this study were previously discussed in section 4.4, specifically sections 4.4.3 and 4.4.6.1. The questionnaire used multiple choice, checkbox and freeform questions to identify a range of data from participants including the usage of passwords, devices, the Internet, potential victims of digital/cyber-related crime and their awareness of both disciplines. The main questions determined for this target group centered on their thoughts of the terms ‘digital forensics’ and ‘cyber security’, and specifically their views on responses to tackling cybercriminal activities through society and policing. These questions were identified as missing avenues in existing research. Responses were thematic analysed to identify themes across views and experiences of cybercrime, discussed in section 4.4.7. The importance of these questions were developed and directed at purposes of rigor and transparency as discussed in section 8.2.1 below. Furthermore, the public participants were asked questions regarding their technologies and security measures by means of identifying current usage and potential experiences of cybercriminal activities.

8.2 The Public Participants

To capture and understand general perceptions of society on digital forensics and cyber security, a questionnaire (see Appendix A – A.6) was distributed across messaging and social media platforms known to the researcher, with the intention to capture viewpoints of the public. More than half of the 102 responses captured were from female participants, and the most popular age for all participants falling between 41 and 55. In terms of employment status, 72 individuals identified as being in full-time employment. The overall highest qualification held by the majority of individuals (n=30) was a Bachelor's Degree, followed by an A-Level or equivalent (n=18). Table B.5.1 identifies the demographic of participants through age, qualifications, and employment status by gender.

8.2.1 The Public as a Stakeholder Group and their Composition

The public may seem an unusual stakeholder group in this study as it looks to capture and assess the experiences and views of those related to digital forensics education, however, inclusion of the public is interesting and useful for evidential quality and, for purposes of fairness, transparency, and rigour in this study. The notion of the public as a stakeholder group grows from the idea of capturing and painting the scene of the overall and wider educational scene for digital forensics and, by extension cyber security. Thus, capturing viewpoints from the public and their understanding of the discipline, and the impact of digital crimes on the society in the wider context is considered important to understanding the wider educational scene. The public are a stakeholder in the educational process, more commonly associated with the wider awareness in business and normal life for example the need for essential cyber security and data knowledge and skills. Awareness of the discipline on behalf of the applicants and their relations may be considered crucial to defining student and public expectations of educational offerings, as discussed in chapter 7.

What must be considered in the inclusion of the public is the potential for social desirability bias among responses (i.e., providing socially acceptable/correct answers). Furthermore, consideration whether such awareness is gained in education or training in regular walks of life, and the affects these may have on the potential to receive informed views. The public respondents in this study are largely made up of female participants (n=62). Furthermore, the group is also largely made up of those who categorise within the age ranges between their 20s and 50s. It may be said that these age groups are relative to the convenience sampling used during the open call for participants known to the researcher and their known contacts and thus the spread of the questionnaire among these age groups. The views of these participants may not be regarded representative of an entire population, this is otherwise unattainable, the use of thematic analysis and data saturation to identify themes among responses are achieved.

While the public perceptions cannot be representative of the entire population, or specific to these instances, they may illuminate and provide a small insight into public perceptions, expectations, observations, and experiences in relation to digital crimes. The public should always be at the forefront of any policy decision. Furthermore, public participants are considered as a stakeholder related to the digital forensic/cyber security education in this study as the underlying purpose of universities are to support and enrich the public through learning and personal development taking into account several social, political and economic factors. Public interest also underpins the necessity to prosecute those who break the law. If the public are disengaged, unaware of apathetic then the underlying system can be questioned.

8.3 Participants' Use of Digital Devices

Accessibility and use of digital devices have grown along with the capacity and functionality of the devices themselves. A report by We are Social (Kemp, 2019) shows that, as of 2019, there are "5.11 billion unique mobile users in the world", an increase of 190 million since 2017 (100 million in 2018 alone). Further to this, there are a reported "3.48 billion social media users in 2019" compared to just "2.56 billion … in 2017" (Kemp, 2017). As previously highlighted, the number of devices easily accessible to an individual is, on average, more than three; where, Figure 8.1 demonstrates the tally of devices utilised among the 102 respondents[66]. Usage of these devices is not necessarily surprising, and participants seem to use a range of devices to access potentially sensitive services online. While these figures are unsurprising they give a small amount of insight into device usage of this sample of individuals. Demonstrating that computers are still among the most popular choices of this group along with smartphones.

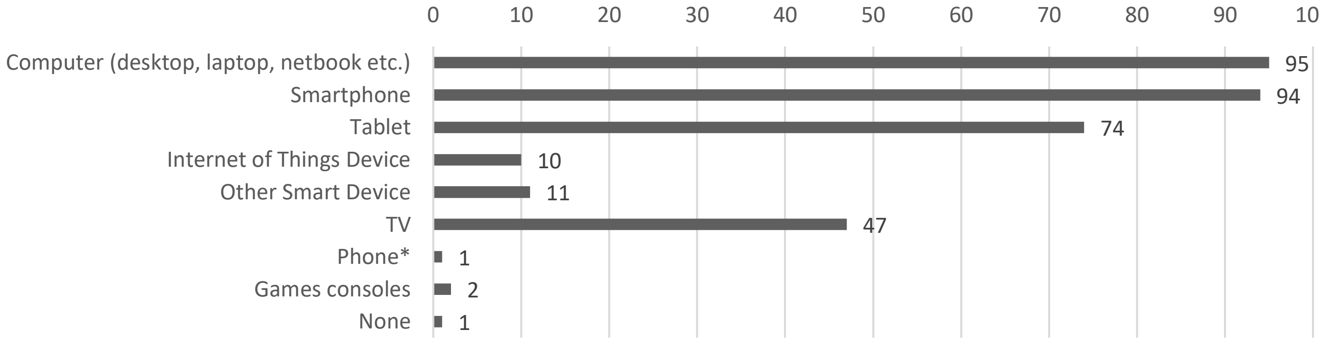


Figure 8.1 – Public Respondents Device Usage to Access Internet

Respondents noted using a variety of devices to access the Internet including more smart-enabled devices, where a TV was among those most popular. The most prevalent activities, where the Internet and digital devices were used, were to Buy Goods (94.1%), followed by Emails (91.2%) and Social Media (89.2%) as depicted in Figure 8.2. Previously, this study highlighted freely available statistics which demonstrate

[66] *Phone with value 1, is not considered due to ambiguity.

mobile Internet usage has overtaken that of the once standard computer worldwide. However, as this questionnaire demonstrates, the usage of both computers (95 responses) and smartphones (94 responses) are equally common of this audience.

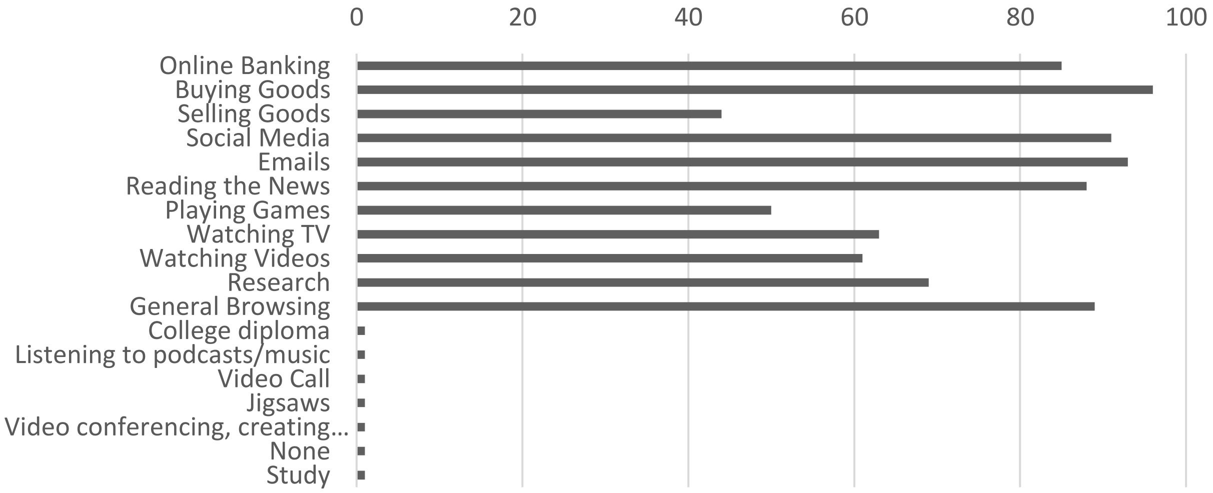


Figure 8.2 – Public Respondents Activities Online

8.4 Participants' Use of Passwords

To identify the importance of passwords to this sample of participants, they were asked two set questions pertaining to the security:

- How often do you change your passwords?
- Have you ever used one of the following as a password? (123456; password; 123456789; qwerty; 123123; google; 111111; qwertyuiop; 1q2w3e4r)

The aim of these questions looked at identifying how the respondents perceive the importance of their passwords. For example, do they use, or have they used, common passwords and do they change their passwords regularly to ensure account security. Passwords are often a key weakness of many simple hacks, for much larger data breaches these security weaknesses are not the target, however, identification of silly passwords, common passwords, and those of insecure length and type are all easy targets for criminals. People's password practices were of interest here due to the abundance of passwords people must use and recollect, often on a regular basis. In particular, the importance of these questions centred on identifying whether people were cautious and wary about their password usage, or whether there were inappropriate practices among the sample of participants, and potential for developed awareness toward information security issues.

Figure 8.3[67] demonstrates a high proportion of individuals who admit they do not change their passwords, approximately 20 percent of respondents. While others identified they change them on schedules between every 3 months and yearly. A common response themed among answers provided in freeform were aligned to individuals changing their passwords when told or prompted to do so, or they had forgotten their previous password or depending on the application, site or device being used.

Figure 8.4 shows that 94 percent of participants recognised they have not used some of the most common passwords known (e.g. 123456; password; 123456789; qwerty; 123123; google; 111111; qwertyuiop; 1q2w3e4r). Social desirability bias must be considered in light of these responses, highlighting the chance that respondents may have been less than truthful about the use of such passwords in effort to provide a more suitable or perceived acceptable answer. However, this cannot be inferred from these results and thus they are used to demonstrate five participants who admittedly used one of these passwords; a small percentage of this sample which is positive.

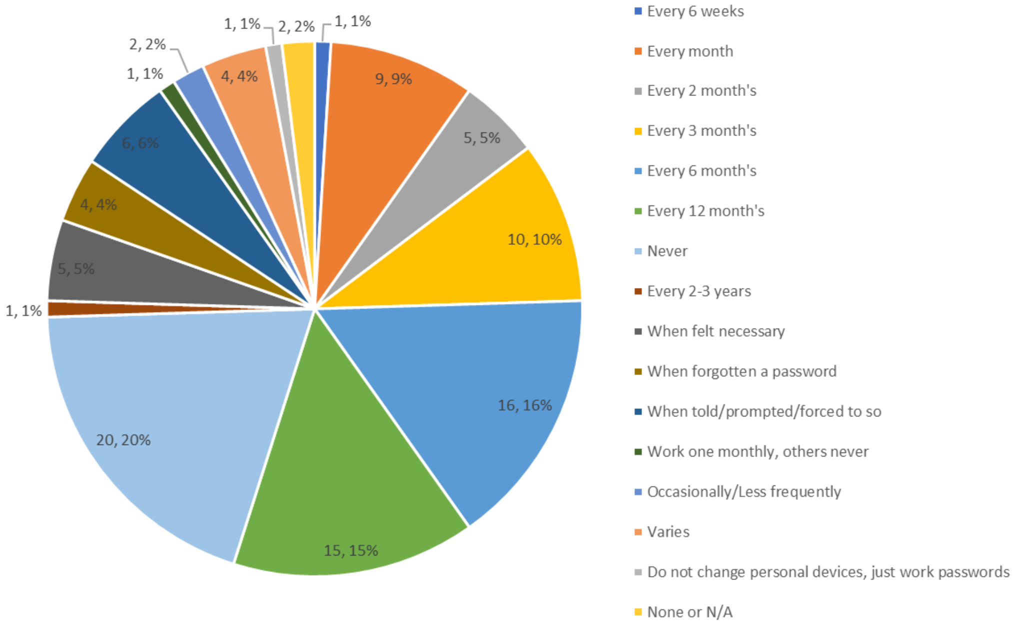


Figure 8.3 – Public Respondents Password Change Schedules (Themed)

Password hygiene is reported by LastPass (2018), a password management company, to be a mixed bag in terms of behaviour and awareness of the public. While the potential bias of this report can be questioned, authors such as, Aytes *et al.* (2003) and Aytes and Connolly (2004) to name a few discuss the importance of human behaviours and tendencies in Information Security and how awareness and education is just one branch in the model for understanding end users efforts toward computer security.

[67] Figure 8.3 and Table 8.4 are linked and replicate participant data.

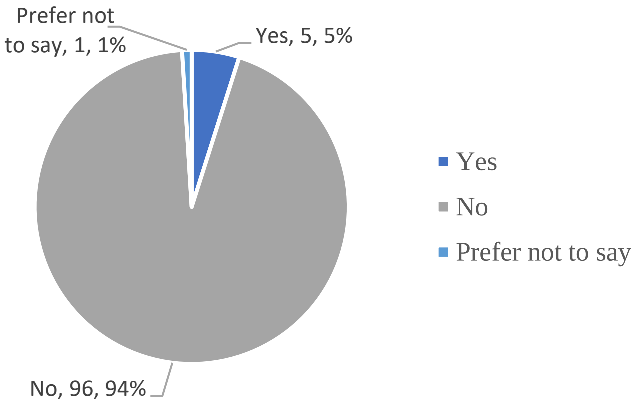


Figure 8.4 – Public Respondents Use of Common Insecure Passwords

It was reported that "91% [of participants] know that using the same passwords for multiple accounts is a security risk, yet 59% mostly or always use the same password" and, that news of a breach does not often entice an end user to change their password (LastPass, 2018, p. 6). A trait of behaviours linking to ignorance and neglect as well as the challenges of creating unique and strong password time after time. These statistics demonstrate that although people may be aware of poor practices, there is still a potential lack of awareness to the importance of password strength and reliance. Of those who have used insecure passwords, three had become a victim of digital crimes (Table 8.1). Although, this study cannot provide concrete evidence to the correlation between participants usage of passwords, age or victimisation.

	Victim of Crime	Not Victim of Crime
18-20	1	0
25-30	0	1
31-40	0	1
41-55	2	0

Table 8.1 – Public Respondents Poor Password Usage and Victimisation

With a greater percentage of participants intimating that they are using more secure passwords, or not admitting to using insecure passwords, the question raised looks towards awareness of criminal activities along with the disciplines of digital forensics and cyber security and their thoughts on crimes to be tackled.

8.5 Participants' Understanding of Digital Forensics and Cyber Security

Prior to distribution of the public questionnaire, the need for questions pertaining to each respondents' view of digital forensics and cyber security were identified as crucial queries. To understand the public image and understanding of each discipline could provide a good starting point to identifying the coverage digital forensics and cyber security has in the public domain, and whether people identify with the image of both roles. Participants were asked two questions:

- What do you think of when you hear the term ‘Digital Forensics’?
- What do you think of when you hear the term 'Cyber Security'?

Analysis of the qualitative data collected for both these questions confirms that some participants are fully aware of what each discipline entails. For example, several respondents relate digital forensics to the “analysis of digital and electronic devices”; “obtaining evidence of activities from (any type of) computing devices”, and “the ability to investigate and recover different materials found on different digital devices especially in relation to crimes”. However, there are also images portrayed by some individuals such as “American TV series”, for example “NCIS” and the characters which mimic and portray digital forensics investigators; coined the ‘CSI Effect’. Much has been written about the effect and its association with the image portrayed of a digital forensic practitioner due to the extensive dramatic licence applied in film and television. This study also identifies some participants recognise and relate digital forensics to one word or one activity; for example, “Banking”; “Crime”; “Forensics”; “Cyber crime”. With one participant stating they are “Unsure”. However, this study highlights that there are only a few participants who hold the image of a ‘CSI Effect’ or one-word association where most participants relate the role to its true meaning.

One respondent defines how the term digital forensics “describes the ability to analyze data left or held on a device like a digital footprint in the same way a crime scene investigator can review a crime”. Yet, another respondent takes a different view akin to something out of a science-fiction novel; albeit, more akin to forensic investigation. This respondent thought of “robots dusting a crime scene for finger prints” when hearing the term digital forensics. Robotics have been used for several years to help with the defusal of explosive devices and in crime scene reconstruction (Se and Jasiobedzki, 2005; Franke and Srihari, 2008), however, the ability for a robot to dust for fingerprints is something for the future of forensic investigations. Both participants clearly make attempts at relating digital forensics in terms of a typical crime scene.

In comparison, when asked what they thought of when hearing the term Cyber Security, similar responses were provided. Where again participants were able to identify crucial aspects of the discipline from “being secure online”; “trying to stop culprits”; “protecting digital assets from unintended access, modification or denial of their use” through to “passwords, personal details” and “OS, application and network security”. Another respondent states they think of cyber security as, “the protection of a computer system or digital device from damage or theft of its software or data and stopping any disruption of any services they may be providing.” Coding of the responses classifies into three key terms demonstrated in Figure 8.5.

Some responses were vague, for instance: “cyber security?” and “computer security”, not homing in on anything specific. While others thought of the term as “complicated”, “Don’t know” and even one respondent noting “Worry”. Where other responses were intriguing such as, “a robot standing at the door of a club waiting to check people's IDs”. This disparate identity of cyber security could prove to outline the true perception of the discipline among members of the public where, some express cyber security as “buzzwords that few understand in any practical sense”.

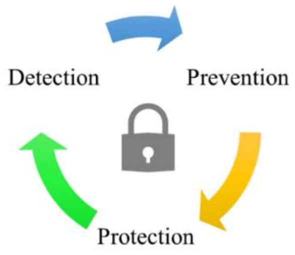


Figure 8.5 – Pubic Respondents View of Cyber Security Categorised

All responses to these questions can be found in Appendix E – E.6 Thoughts of Participants of the Terms: Digital Forensics and Cyber Security.

8.6 Participants Fallen Victim: A Comparison to Official Statistics

Of the 102 participants, 25 recognised having been a victim of a digital/cyber-related crime, 1 of minor crime (spam), a total of 26 victims, and 1 who stated: “almost when a guy called for the other half of my online banking details”. Leaving 75 individuals responding “no”. With nearly 25 percent having been a victim of digital crime, further analysis into how the victims responded and their views on what needs to be tackled. It also shows inherently that there are continued concerns surrounding the understanding of cyber security, digital forensics and the further need for education, both for the development of successful practitioners and for the public as users in defending themselves sufficiently against digital crimes.

With 75 “no” responses, it is apparent that some of the participants in this study have either not fallen victim of, or have protected themselves to a suitable degree against, digital/cyber-crime. However, of those who have fallen victim, 60 percent were that of bank card/online banking fraud, followed by phishing attacks (32 percent) and online fraud of goods (e.g., goods purchased but not delivered/counterfeit) (28 percent). Figure 8.6 depicts single and multiple instances of crimes, or subsequent criminal activities, for which 25 individuals categorised they had fallen victim.

Victims were asked how they responded to the crimes; for example, did they report the crime and the outcome. Responses included contacting relevant banks and email service providers to investigate and, for a fix to the incident. Often, the issues were resolved with little damage or loss to the individuals. One respondent noted that they "lost £0.02 thanks to the quick thinking of [their] bank", while others noted they were "refunded", any "black marks … were erased", while others included an employee/"insider" being sacked or sites closed.

Other participants expressed their interest in responding through learning how to defend themselves; one characterises their response with efforts placed in "becom[ing] a keyboard warrior & learn[ing] basic digital self defense/preservation". However, term 'keyboard warrior' is coined as an informal noun to mean someone who displays aggressive tendencies and posts in an online setting, while concealing their real identity (Cambridge University Press, 2013). It is understood that this is not what the respondent means, and that they are in fact vocalising their own needs, as well as others, to become more skilled to defend themselves and implement security mechanisms on devices and online.

With another stating they "step[ped] up all online passwords using random strings saved using external software installed on [their] computers and smart devices (the latter of which requires fingerprint authorization)". This shows that, in some cases, individuals are educating themselves in ways to prevent being a victim to such crimes again.

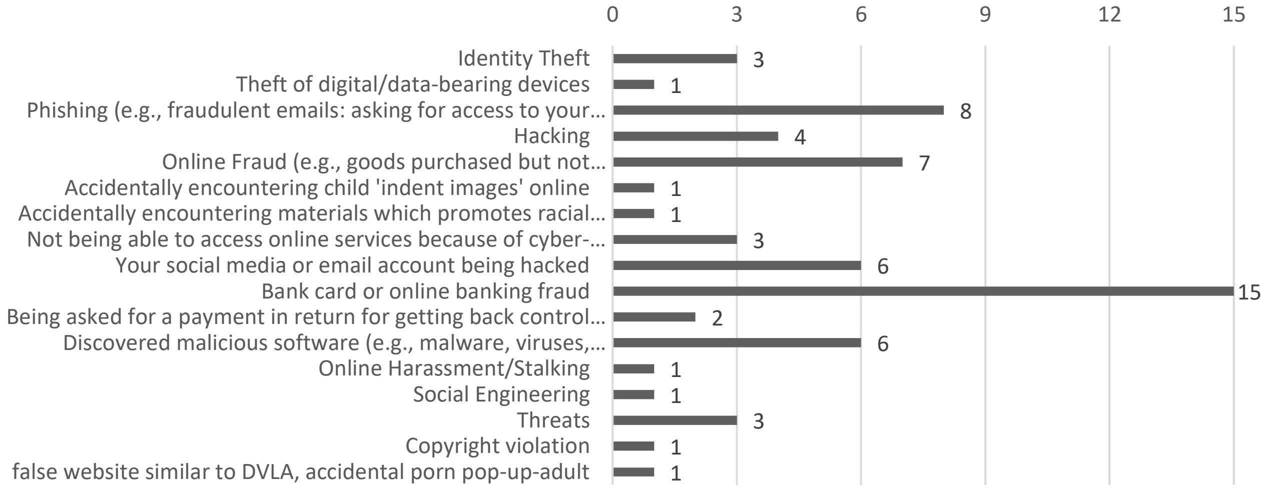


Figure 8.6 – Public Responses as Victims of Digital/Cyber Crime

Results show that 17 victims reported the crime to the relevant authorities, some resulting in the identification of criminals and leading to arrests, while others were fully reimbursed, and all issues resolved. This left nine individuals (~35 percent) who did not report the crime, supporting the belief that there are greater possibilities and costs associated to digital crimes due to unknown and unreported crimes. To support this claim current statistical evidence from relevant sources such as the Crime Survey for England and Wales (CSEW), National Fraud Intelligence and Action Groups are discussed below.

8.6.1 England and Wales Crime Survey Results

The latest results, ending September 2017, from the Crime Survey for England and Wales (CSEW) find estimates to be much higher than other known bodies where, it is recognised "the [CSEW] survey is able to capture a large volume of lower-harm cases that are less likely to have been reported to the authorities" (The Office for National Statistics, 2018b). The methodology behind the CSEW survey takes a face-to-face interview approach with people in England and Wales, where core victimisation questions focusing on several types of crimes are pursued. An approximate 35,000 household representation is expected year-on-year as of 2012/13 survey (The Office for National Statistics, 2018d).

Originally the CSEW focused on traditional crimes within England and Wales such as, household robberies, violence and fraud. However, with the increase in use of the Internet and its associated crimes, the demand for official statistical evidence of related crimes is desired. Thus, between October 2015 and September 2017, the national survey introduced questions related to fraud and computer misuse. These questions were directed to just half the survey sample; from October 2017 it is reported these will be rolled out to all respondents. With the survey coverage accounting for only half the sample, there are still questions as to the additional number of unknown digital/cyber-related crimes suffered by individuals.

The National Crime Agency (2016) note that "[u]nder-reporting [of cyber crime] continues to obscure the impact of cyber crime on the UK". Further analysis by the CSEW shows "that only 14% of incidents of fraud and computer misuse either come to the attention of the police or are reported by the victim to Action Fraud" (The Office for National Statistics, 2018c).

Results of the CSEW survey also show there to have been approximately 4.7 million fraud and computer misuse incidents classified ending September 2017; demonstrating a slight decrease on the previous year (The Office for National Statistics, 2018b). The reports of these activities being related to cybercrime are predominantly high, where "[o]ver half of fraud incidents … were cyber-related … [at approximately] 1.8 million incidents" (The Office for National Statistics, 2018b). Furthermore, the highest proportion of loss due to fraud was associated with "Bank and credit account fraud", accounting for nearly 2.4 million incidents with over 2 million victims. A similar trait is represented by the study in this thesis, demonstrating there is still much progress to be made with respect of fraud and online banking. In terms of crimes related to computer misuse, the CSEW highlights that over 900,000 (64 percent) of incidents were related to computer viruses and over 540,000 incidents (36 percent) were associated with unauthorised access to personal information (which included incidents of hacking) (The Office for National Statistics, 2018a).

In comparison, the smaller scale study conducted in this thesis shows individuals classify crimes as several incidents (Figure 8.6 above), with 4 incidents of hacking, 6 as having discovered malicious software, 8 as phishing and 7 as online fraud in retail (e.g. goods purchased and not delivered or of counterfeit nature). Although a smaller representation of the public, a greater percentage of respondents reported the crime to relevant authorities in comparison; demonstrating an awareness among this sample and the need for reactive responses.

8.7 Public Awareness

It is apparent that a majority of members of the public are aware of the potential for digital crime. For instance, one respondent noted they were almost a victim of such crimes

> "when a guy called for the other half of my [the participants] online banking details. He pretended to be from [the bank] but [the participant] knew they wouldn't ask [them] certain things. So [the participant] called [the bank] and [the bank] confirmed it wasn't them."

Others who fell victim of successful crimes noted end results meaning they had to "change [their] phone login details, cancel[their] online bank account and received a full refund from [the] bank"; "resolved and money returned"; "no damage, quick action taken".

While others were not quite successful with results; one respondent aged 31-40 reported crime(s) to what they felt was the relevant authority/websites and noted "[n]o one was interested. Nothing. Lost money." This respondent recognised crimes to have occurred such as;

> "Phishing (e.g., fraudulent emails: asking for access to your computer, logins, money or personal details), false website similar to DVLA, accidental porn pop-up-adult."

Looking deeper into the end result of many of these incidents found among the participants, led to a response echoed by many for the need of wider awareness and education of digital crimes and cyber security. Several people note having learned from the crime or from their own mistakes. One example of this is a respondent aged between 25 and 30 who fell victim to what they categorise as several incidents:

> "Online Fraud (e.g., goods purchased but not delivered/counterfeit), Not being able to access online services because of cyber-attacks, your social media or email account being hacked, Discovered malicious software (e.g., malware, viruses, trojans) on your device, Threats"

Although, rather unlucky, but entirely plausible, to have fallen victim to all incidents, it is not uncommon. A curiosity surrounds whether people realise they have been attacked in similar circumstances across all generations; a wider study is required to discover this. However, the National Crime Agency (NCA) (no date) note that "[m]ore and more teenagers and young people are getting involved in cyber crime" noting reasons such as, the excitement and fun attached to crimes including unauthorised computer access, production and distribution of malware and Distributed Denial of Service (DDoS) attacks through to individuals being unaware and unacquainted with the consequences and penalties of such crimes.

The respondent continues by expressing their view that society should be trying to tackle digital crime and cyber security through "Education, Education, Education". Expressing how they believe there are "[s]o many people [who] don't understand digital crime" and that in their circumstance, they "secured all [their] accounts regardless of the type of breach that occurred, and you learn from your mistakes."

While the need for more awareness of crime and prevention are shown, there is also the need for education and awareness to combat the fear and worry these incidents invoke. One respondent aged 41-55 identified they had become victim to attempts or successful incidents, ranging from:

> "Phishing (e.g., fraudulent emails: asking for access to your computer, logins, money or personal details), Online Fraud (e.g., goods purchased but not delivered/counterfeit), Discovered malicious software (e.g., malware, viruses, trojans) on your device"

They responded in the case of success using what they describe as a "Virus killer" which led to "deletion" of the viruses, which they then reported; however, they are now "dubious of us[ing the Internet]". Although, they were the only respondent and victim of a crime to express a level of anxiety towards further use.

Another response took a different meaning to digital forensics stating they thought of the "[u]se [of an] incognito browser & [to] Hide [their] laptop" when hearing the term digital forensics. When hearing the term cyber security, they thought "[their] laptop isn't up to scratch". Having been a victim of a crime, it is a wonder if this is anxiety driven due to victimisation. The respondent noted crimes such as:

> "Theft of digital/data-bearing devices, Phishing (e.g., fraudulent emails: asking for access to your computer, logins, money or personal details), Hacking, Accidentally encountering materials which promotes racial hatred or religious extremism, Not being able to access online services because of cyber-attacks, [their] social media or email account being hacked, Being asked for a payment in return for getting back control of

> [their] device, Discovered malicious software (e.g., malware, viruses, trojans) on [their] device, Social Engineering, Threats"

The participants "stolen devices [were] recovered … computer av cleaned, passwords changed etc.", there is clearly still some anxiety in the use of, and continued presence of "phishing emails … weekly" and concerns over the "religious & ethnic hate groups websites still [being] active because they got protected by free speech". This is the very same participant whose response was to learn the basic digital self-defence skills and become a "keyboard warrior".

What this questionnaire also shows is it does not matter what age or gender you are, you can fall foul of a digital crime at any time; albeit on a small sample of data Table 8.2 shows the demographic of people who fell victim of a crime. A majority of those who fell victim in this study are aged between 41 and 55 (Table 8.2[68]); the same majority age group who completed this questionnaire. Although responses to this question are not exhaustive nor representative of all individuals aged 18 to 30, this study demonstrates that even those who are technologically aware can become victim of digital/cyber-related crimes. Or, they are at a minimum more aware of what digital crime is.

Characteristics	Male n	(%)	Female n	(%)	Other n	(%)	Total Victims n	(%)	% of Total Respondents by Age
Age									
18-20	3	(30.0)	0	(0.0)	0	(0.0)	3	(12.0)	75
21-24	0	(0.0)	3	(21.4)	0	(0.0)	3	(12.0)	37.5
25-30	3	(30.0)	1	(7.1)	0	(0.0)	4	(16.0)	19
31-40	0	(0.0)	4	(28.6)	0	(0.0)	4	(16.0)	23.5
41-55	3	(30.0)	5	(35.7)	1	(100.0)	9	(36.0)	27.3
56-65	0	(0.0)	1	(7.1)	0	(0.0)	1	(4.0)	9
66+	1	(10.0)	0	(0.0)	0	(0.0)	1	(4.0)	12.5
Total	10	(100.0)	14	(100.0)	1	(100.0)	25	(100.0)	(24.5)
Gender	10	(40.0)	14	(56.0)	1	(4.0)	25	(100.0)	-

Table 8.2 – Public Respondents: Demographic of Victims of Crime

With greater use in devices, the Internet and number of crimes carried out online or using digital devices, supports the ever-greater need for practitioners within the disciplines seeking to combat digital crime (e.g., the need for effective digital forensics and cyber security practitioners).

[68] Table 8.2 is used to identify those who recognised they had fallen victim to some crimes. It demonstrates their password usage and finds that it does not matter what age or potential awareness you may have about or with technology that you can become a victim of digital crimes.

8.8 The View of the Public: What should be tackled in Society?

Several responses to this question highlight the need for society to understand the nature of digital forensics and cyber security, along with the awareness and the image seen of a digital forensic practitioner. One respondent stated we should be looking to tackle "[t]he image of a forensics analyst … [they] are not NCIS … keyboard hackers." Another respondent stated "raising the profile of cyber/digital crime to show it is not victimless" is crucial, as well as "raising the awareness of how to protect [oneself] from digital and cyber crime. Providing free confidential and reliable advice to victims of cyber crime."

A respondent aged 25-30, who has not been affected by digital crimes, summarises the need for "an established mid-ground where the Internet can be used properly", expressing how,

> "the digital age has made it far more easy for people to negatively impact people's
> lives while at the same time being a valuable asset in people's lives."

Similarly, another respondent states "awareness [is required] that this is a new and growing problem and the [need to address the] general attitude of those who consider it a lesser crime compared to its physical counterpart." This is an interesting perception, which many have picked up on while identifying how they feel society are happy to place less emphasis on their personal data online and on devices than maybe reflecting on the traditional use of paper and keys for information and storage, Where, "awareness among general society of the vulnerabilities needs to be improved, and the possible consequences to individuals affected made clearer."

This impact and a greater understanding of threats needed is depicted by many respondents, identifying a strong consensus for the need to educate people in preventative measures, potential criminal acts, the associated affects and responses required. One respondent stated they feel "teaching 3 stages of defence: prevention, incidence management, consequence management" are central to tackling society's approach to security and online information. While others focus on education at earlier stages in society; for example, "schools need to teach children more about [digital crime]" and "education at home & in schools". However, it is not just awareness by the end users that participants call into question, with responses such as, tackling "the actual source of criminal activity".

Furthermore, the respect towards others and the need for more transparency is highlighted in who and what data can be accessed, collected and used. Although a majority of responses are in relation to understanding what a criminal can access in terms of data on the individual, one respondent notes the need for "transparency" in terms of the data law enforcement can access. Where they state, "more transparency in who has access to what information – so we know what the govt/police etc., take from us [and] know from us." Broadly speaking however, there is a trade-off between that amount of data which can be obtained, the length of time it takes as well as how intrusive the examinations.

Often, concerns are targeted towards what multiple businesses or institutions hold in terms of Personally Identifiable Information (PII), (particularly heightened with the recent introduction of the General Data Protection Regulation (GDPR) – discussed later) and the potential for malicious access to such data. However, as seen with the Investigatory Powers Act 2016 (The Stationery Office, 2017), nicknamed the Snooper's Charter, there are more and more concerns over the lawfulness of mass data surveillance by government and public service departments. Security services and official agencies under the new legislation have the right to access and hack into communications, including bulk data. The government expresses the need for such measures due to times of heightened security threats. Therefore, it is no wonder why some, like the individual above, appear to show particular anxiety towards the collection of data by law enforcement and government departments alike. Although it should be noted that, collection of such data can aid investigations into criminal offences and state attacks. Nevertheless, restrictions and precautions to accessing, and the right to access, such information should be of utmost priority.

Another respondent expresses the need for "less sweeping powers by the state" and the requirements for "updating appropriate legislation" to combat issues such as "Cyber bullying, copyright issues, self-censorship and the 'social cooling' effect" where they believe there needs to be a "mass education of 'cyber sec' from a young age". In contrast to the views for less sweeping powers and downplay in the role of investigatory powers, one respondent portrays the view that "[e]verything above! [(i.e. mentioned within the questionnaire should be tackled), they] think digital crime is only going to get worse and at the moment, the police are perhaps a little ill-equipped to deal with this." This point makes for interesting discussion and shows a level of mindfulness of the position, particularly in public sector roles toward resourcing, staffing, funding, skills and time.

Other points raised by several participants which also make for a contrasting point to anxieties shown toward too much 'snooping power' (e.g., what data governing bodies are able to access) are the need for greater controls, more monitoring and policing and the development of stronger penalties and punishments. Responses included the need for:

- "stricter monitoring or access to sites";
- "stronger penalties";
- "more visible policing of sites";
- "harsher punishment of identity thief and the ability for the police to gain access if reasonable proof can be provided";

- "better public awareness. Tighter controls online & less anonymity online, not for the average user but for advanced users like those who use the Dark Web";
- "need to pursue hackers more aggressive";
- "motivations or perpetrators to reduce risk, training and education, certifications in relation to devices";
- "cyber bullies should be able to be barred from the internet for all uses.....that would be a good punishment as a min up to and including jail time".

Table 8.3 demonstrates these points under the theme of Crime and Punishment (26 occurrences). It could be argued that several items listed above might not be necessary if, as a society, we could tackle – through education, the motivation to commit a crime. However, committing a crime, i.e. an unlawful act, has long existed, both with and without the addition of technology where education, nor reformation, has been able to fully diminish peoples' motivations. The vast depth and breadth of the Internet has only enhanced the capabilities of criminal activities in other dimensions and resources. This begs the question, what can people in society, professionals, governments, and bodies do to tackle this.

Coded Grouping	Category	Total Count (Category)	Total Count (Group)
Tackling in Society			
Knowledge	Awareness	43	71
	Education	25	
	Training	1	
	Support	2	
Crime & Punishment	Crimes	17	26
	Punishment	3	
	Criminals	6	
Control	Policing	3	11
	Monitoring	2	
	Transparency	2	
	Responsibility	2	
	International Cooperation	2	
Society	Social Media	1	7
	Image of Practitioners	1	
	Respect	4	
	Other	1	
Security & Prevention		19	19
Everything		3	3
Other	Unsure	6	8
	No Response	2	
Total		145	145

Table 8.3 – Coded Public Responses on what society should tackle in digital forensics/cyber security

One respondent comments "[t]here is so much freedom for all users on the Internet. I really do not know what can be done"; with another stating, "I wouldn't know where to start in answering this". This is not surprising; however, Table 8.3 shows only 8 occurrences where people were unsure or did not know what should, or could, be tackled within society. This is interesting as participants within the survey identify responses which show a conscientious nature toward the need for change and response to security issues. Responses from the public were open coded into categories which most suited the items stressed e.g., education, specific crimes and punishments, these were then categorised into groups of similar topics (as depicted in Table 8.3).

Security was another theme which resonated among participants. The theme included responses homing in on the concern that "Security risks are not taken as seriously as they should be" and that people needed to become accustomed to the preventative techniques they can use to help secure their devices and systems. These responses were grouped into Security and Prevention. Some people noted that there specifically needs to be more support and availability of information for much older generations to understand the Internet, devices and security. More commonly, security coded responses linked to knowledge (i.e. people being more aware of security measures and educated to protect themselves). Security, also, for some respondents linked to stronger punishments for criminals accessing and distributing information where one respondent discusses security is not just about people's device security but data security, articulating;

> "Websites are more secure and harder to hack, it's becoming more common for information to be leaked and personal identities stolen."

Although there is no definitive statistical evidence to prove or refute the participants claim that hacking a website is much harder in the current day Internet. In fact, the rise in data breaches, ransomware and cryptocurrency-themed attacks highlight the need for better security all-round. Be it a website, business premises, servers, networks or otherwise. Findings from the 2017 Breach Level Index (BLI) Report show that more than 2.6 billion records were breached in 2017 (Gemalto, 2018). The Information Commissioner's Office (2018b) publish information on breaches reported within the UK each quarter; statistics for data breaches in the fourth quarter of 2017/18 saw "957 reported data security incidents [...,] a 17% increase on Q3 (815 reports)". It is believed that the recent increase in reports "are possibly due to increased awareness of the GDPR [where data breaches must be reported within 72 hours] and the launch of [the ICO's] new Personal Data Breach helpline" (Information Commissioner's Office, 2018c). The participants point regarding the leak of information and potential for personal identification theft is of concern; people need to be aware and mindful of the severity and consequences.

Table 8.3 stresses the vast and most profound opinion among respondents as that of awareness and education, where coding found these as the overarching theme with 68 occurrences. Results so far have shown that people believe there needs to be more awareness of the crimes, security flaws and measures and more. Thus, discussions were coded under the grouping: knowledge. Many of these were associated with the wider need for awareness among members of the general public.

Numerous respondents discuss the need for the awareness of vulnerabilities and crimes as well as "the general understanding of technologies and the dangers involved". Seeking a way for people to better protect themselves and their information as a crucial focal point for these participants. One participant epitomises this stating, "more efforts should be put into education regarding the general Internet hygiene, phishing, viruses and the dangers associated with these to help in prevention". Another respondent acknowledges the general unawareness and unfamiliarity, writing:

> "Making people in general aware as to how easy it is to gain information on them. How liberally people use the internet without realising they could be passing on their information unwillingly."

Further to the education of adults, many respondents pinpoint the need for education targeting a much younger and inexperienced age group. Where they believe schools should teach and "involve younger generations in digital crime prevention" to protect the adolescents from sharing too much information, and from crimes such as, cyber bulling, abuse and harassment.

One respondent, male aged 41-55, expressed concern throughout their responses towards the vulnerability of the younger generations. In addition they emphasised an interesting point of view on the need for responsibility. The respondent writes:

> "Education at home [and] in schools. More responsibility placed in the hands of those making millions out of the internet. YouTube Google Bing Facebook, they're very happy to take our money but they don't provide sufficient protection."

This is an interesting debate of where the responsibility lies, and to what degree the responsibility should be weighted to Internet-based companies, the criminals, the victims and governing authorities. This study does not look to answer this question in-depth due to its vast breadth and uncertainty. However, at the time of writing, there have been several news stories such as, the Facebook and Cambridge Analytica scandal (Information Commissioner's Office, 2018d) which have heightened the need for companies to take responsibility for actions. Other stories include the fine to Google (Alphabet Inc.) on strengthening its position in the business of search engines via illegal and unethical means (under the EU antitrust rules)

(European Commission, 2018). Linking to the point of responsibility and transparency in the collection and usage of customers data. Consumer trust is centred around ensuring personal data is secure and an argument for transparency in data use, particularly when it is almost inevitable that data breaches will occur.

In a report by the UK Department for Culture, Media & Sport (2018), "778 businesses and 218 charities" identified a breach or attack between 2017-18; where 28 and 30 percent respectively did not take further preventative actions. Top reactions following these violations included measures such as,

- antivirus or anti-malware measures (22% and 19% respectively);
- knowledge (e.g. staff training, communications and awareness) (18% and 13% respectively);
- system configurations and updates (15% and 7% respectively);
- policies and procedures (9% and 15% respectively); and
- outsourcing security measures (5% and 2% respectively).

— (Department for Culture, Media & Sport, 2018, p. 50)

Arguably, the less than reactive response of some businesses and charities calls for and supports an argument for greater transparency and accountability/responsibility. However, the appointment of responsibility should also be targeted at the general public in a) securing their own data where possible, b) awareness of company privacy and security policies, and c) the avoidance of general ignorance to the Internet and its vulnerabilities. Again, supporting the need for awareness and education in certain aspects of computer and cyber security for both end user and companies.

One respondent picks up on the need for education in 'cyber', due to its nature of being intangible, particularly referring to the use and security of passwords. They voice the concern that "education [is required], because 'cyber' is not tangible, people care less about their passwords than house keys." The results from this questionnaire support this claim, presenting 20 respondents who "Never" change their passwords. That is 19.6 percent of the sample. Table 8.4 demonstrates the schedule for which the 102 respondents admitted to changing their passwords.

As depicted in Table 8.4, along with those who never change their passwords, 15 respondents (14.7 percent) change their passwords on a yearly basis; 16 individuals (15.7 percent) on a 6-monthly basis; 10 respondents (9.8 percent) every three months; 5 individuals (4.9 percent) every two months and 9 respondents (8.8 percent) every month. Nevertheless, do they remember or change all their passwords? Abovementioned were attributes highlighting human influence on computer and Internet security including behaviours which influence password validity and security which can, and will, be exploited. Emphasising the human element within digital crime and cyber security. There have been numerous reports, summarised by Kennedy

(2016), reporting a vast sum of business and personal passwords which individuals have to recollect, ranging from 6 to 207 accounts and passwords.

Characteristics	Male n (%)		Female n (%)		Other n (%)		Prefer not to say n (%)		% of Total Respondents by Password Schedule	
Password Schedule										
Every month	6	(15.7)	3	(5.1)	0	(0.0)	0	(0.0)	9	(8.8)
Every 2 months	0	(0.0)	5	(8.5)	0	(0.0)	0	(0.0)	5	(4.9)
Every 3 months	4	(10.5)	4	(6.8)	1	(25.0)	1	(100.0)	10	(9.8)
Every 6 months	8	(21.1)	8	(13.6)	0	(0.0)	0	(0.0)	16	(15.7)
Every 12 months	4	(10.5)	10	(16.9)	1	(25.0)	0	(0.0)	15	(14.7)
Never	8	(21.1)	11	(18.6)	1	(25.0)	0	(0.0)	20	(19.6)
Other	8	(21.1)	18	(30.5)	1	(25.0)	0	(0.0)	27	(26.5)
Total	38	(100.0)	59	(100.0)	4	(100.0)	1	(100.0)	102	(100.0)

Table 8.4 – Public Respondents Password Change Schedule

Further analysis of participants in this questionnaire demonstrates a high proportion (26.5 percent) of people who changed their passwords infrequently. Many noting that they only change passwords when they have forgotten their latest one; with responses such as:

- “only when hacked or if I cannot remember my password”
- “when I forget them!”
- “when I feel I have to, need to, have forgotten previous one”
- “when I have forgotten the one I was using before”
- “less frequently”

While others are reliant on systems and procedures in place which force them to change passwords. Many respondents express they only change their passwords “when required by systems” (e.g. work passwords). The heavy reliance on systems and policies to tell a user when to change a password is often only beneficial in, for example, responses such as these:

- “when I have to as told to me by the website / program I am using”
- “when asked to. I am very bad at this!”
- “when I'm forced to.”

While some admit they are poor with their passwords, others are ignorant or uneducated to the importance of a secure password. One respondent states they “don’t change passwords on [their] personal devices just on the computers [they] use at work". This is not a trait among one individual in this questionnaire, with another stating, "work one monthly, others never". This is a serious cause for concern, where there seems to be little transfer of learning of password security between the workplace and home. Other responses range from it "varies on what it's for" to "whenever...". There are several participants whose response is to change their password when they feel it is necessary considering and "depending on what site/app the password is used for." This attitude is more promising.

Looking to business password protocols, companies have now been advised against traditional password schedules such as monthly to six-monthly password change cycles; where the Communications-Electronics Security Group and Centre for the Protection of National Infrastructure (2015, p. 6) recommend they should "only ask users to change their passwords on indication or suspicion of compromise". For the users benefit of recollecting their password along with many others, the agencies note that password iterations will only see "minor variations" and that a compromised password will "generally be exploited immediately" (Communications-Electronics Security Group and Centre for the Protection of National Infrastructure, 2015, p. 6). However, businesses can monitor and detect unusual logins as well as instantly notifying the user of the need to change their password; the same cannot be said for the regular computer/Internet user at home. Demonstrating the need for wider awareness and education of security outside the workplace.

8.9 The View of the Public: What Online/Cyber Crime Should Law Enforcement be tackling?

So far, this study has highlighted the views of participants in terms of what needs to be tackled in society, however, this begs the question "what online or cybercrime do [they] want and expect police officers to be tackling?". Respondents have so far noted the need for awareness and education and further, some have identified having been a victim of crimes such as fraud, hacking and theft. However, the next stage of this research identifies the expectations and views of public respondents toward activities which they believe should be prioritised by law enforcement. The UK Cyber Crime Strategy (Home Office, 2010) pinpoints the need for government departments "to provide leadership in responding to cyber crime at a policy level" identifying several crimes, key aims and intentions to enhance the fight against threats.

As such, this led to the identification of, and the need to understand, priorities which individuals expect police officers to be tackling relating to online and cybercrime. Participants were asked for their views in the broadest of terms (e.g. looking at 'police officers' rather than specific to digital forensic or cyber security practitioners). Due to the ever-growing nature of digital devices and associated crime in digital and ordinary crimes, as well as much larger and organised crimes, it is recognised that digital and online traces are used in multiple facets throughout investigations within law enforcement. Thus, the question recognises this and allows for respondents to be open with their response.

Several key interests were identified among respondents; where, one participant did not respond. Several responses were relatively vague; for example, "All of it"; "All"; "All Cybercrime"; "Anything that is meant to harm people" and "All! It is a crime". A total of 24 responded with this type of response.

Other responses find some participants expressing "I do not know enough" or "do not understand" cybercrime to be able to answer the question. A total of 3 voiced this; again, emphasising the need for continued public awareness-raising towards security, crimes and victimisation.

For example, the UK Cyber Crime Strategy identifies issues with the reliance on out-of-the-box security with respect of technological devices and assumptions made when accessing the Internet. Narrating that how people access the Internet, "often from the comfort of the home or office, may lead to a relaxing of the awareness of threats that would not be the case if a person was offline" (Home Office, 2010, p. 11). Although, the strategy does identify the increase in public awareness-raising in times where "attacks are becoming increasingly sophisticated" (Home Office, 2010, p. 13). They highlight this is continuous with multiple online crimes growing and evermore prevalent today.

To identify the topical and most important crimes responses were coded by criminal activity mentioned and tallied. Each category was then founded through the grouping of crimes; for instance, 'Theft' included identity theft/fraud, theft of data and, any instance where theft was singularly mentioned. Many of these categories were founded taking into account crimes outlined in Section 3.3 of the UK Cyber Crime Strategy (Home Office, 2010, p. 11). The strategy highlights crimes such as: financially-based crimes (e.g., online fraud, identity theft, intellectual property theft and data security), as well as non-financial crimes (e.g., threats to a child, hate crimes and political extremism). All of which are noted in responses from participants of the questionnaire in this thesis.

Table 8.5 depicts each category and the corresponding crimes, also highlighting the number of instances where one or multiple crimes were mentioned by participants. Nine main categories were identified. Results show, identity theft/fraud (n=25), fraud (n=22), hacking & hackers (n=16), cyber bullying (n=11) and grooming (n=9) were most notable mentioned crimes which law enforcement should prioritise in their efforts to tackle online crime, according to respondents.

Category	Voiced n Times	Crimes Grouped
Child Crimes	36	grooming, child pornography/abuse, child exploitation, paedophiles, indecent/illegal materials
Financial Loss & Banking Fraud	16	financial loss, bank fraud, money laundering
Fraud	23	fraud, insurance fraud
Hacking & Hackers	18	hacking, hackers, account take over
Malicious Software	4	ransomware, viruses
Scams	6	phishing, scams, fake websites and fundraisers
Terrorism	7	terrorism, anti-terror activities and communications
Theft	32	ID fraud/theft, theft, data theft
Violence & Abuse	24	cyber bullying, harassment, hate speech/crime, discrimination, trolling, doxing/personal defamation

Table 8.5 – Public Respondent Views of Crimes Law Enforcement Should Tackle Grouped

Figure 8.7, an adapted version of the Whittling Wedge diagram (Duncan, 2018), demonstrates the crimes categorised by high to low importance (i.e., number of times voiced in the questionnaire) which this sample of respondents relate to in terms of cybercrime, and tackling such crimes.

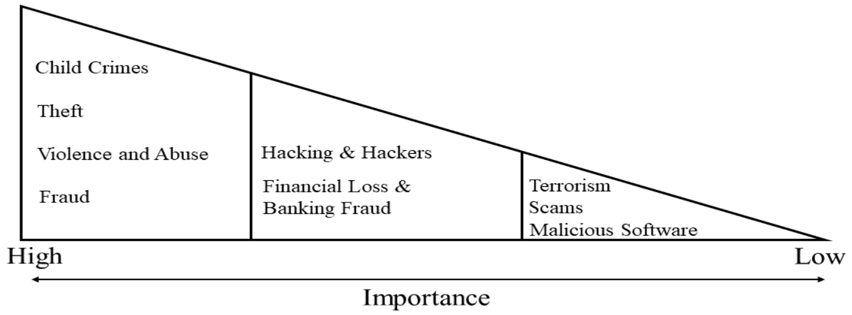


Figure 8.7 – Public Respondents Views on Online/Cyber Crime Police Officers Should be Tackling

Data security, the awareness of preventative measures, and the awareness of online crimes were, again, mentioned by participants. One expressing how they felt law enforcement should be tackling "any criminal activity via digital means [and] helping give crime prevention advice and assistance."

On the other hand, there were several individuals who noted all crimes should be tackled, while recognising that tackling all online/cyber-crime "is not a credible reality". A few respondents even epitomise the view that some crimes are more important than others (in their opinion). For example, answers such as those listed below were provided:

- “As much as possible, from areas like child exploitation and fraud to simple "trolling" of people for no reason”;
- “All crimes. For instance; theft of all kinds (including identity), harassment, selling of illegal goods, etc”;
- “All of it! identity theft and fraud as priority”.

A smaller set of responses made were unable to be categorised within the above nine categories and were left uncategorised. For example, responses which were lengthier and more specific in depth such as an answer from one participant who expresses their views on the role companies play in data loss and security:

> “Ideally all of it! Realistically, I think corporate negligence over data and financial losses probably results in the greatest actual harm to the most people and I think companies who experience such losses (whether through poor cyber security practices or through incompetence) should not only be more heavily fined, but relevant individuals should face prison sentences as well.”

Although this response could have been categorised under data theft, the researcher felt this response highlighted more than a type of crime and expressed opinions pertinent to the need for accountability of businesses, and not just members of the public. Up until now, the image of digital forensics and cyber security has been considered where in most instances these have coaligned with education and training and public-awareness-raising. However, as described in the response above, the culture of security and the role/responsibility of governments, public-sector and private industry should be considered. The above respondent expresses the need for responsibility to be defined, i.e., who is responsible in corporate financial and data loss quandaries. The participant stresses the need for far more and greater sanctions in terms of penalties (e.g. fines, liability for damages and custodial sentencing). Although this is not as straight forward as described, particularly where fines or imprisonments do not fit all crimes in all investigations.

In most recent years, there have been many cases where fines have been issued due to mass data loss. Several types of crime with respect of data loss are considered, ranging from the loss of a device through to large cyber-attacks resulting in relatively large impacts on members of the public and businesses alike. According to analysis conducted by PricewaterhouseCoopers (PwC) (2017), the number of data enforcement actions over the past years has increased, where “23 … were issued in 2016 … [compared to] nine notices issues in 2015". Further to this, PwC's analysis found double the number of fines served reaching a total of "thirty-five fines totalling £3,245,000" (PricewaterhouseCoopers (PwC), 2017).

Back in 2014 the UK saw the data loss of thousands of prisoner records, due to the loss of a hard drive, where The Ministry of Justice was fined the sum of £180,000 for "serious failings in the handling of confidential data" (Cellan-Jones, 2014), this was not the first time such records had been compromised either. Similarly, The Greater Manchester Police were served a £150,000 fine after unencrypted "DVDs containing footage of interviews with victims of violent or sexual crimes" went missing in delivery to a section within the NCA (Information Commissioner's Office, 2017).

Serious failures have been observed for large companies such as TalkTalk, Yahoo and Sony where news reports have highlighted significant cyber-attacks and loss of personal information. Customers of TalkTalk were left worried and anxious when the company reported, in 2015, they were aware they had become victim of cyber-attacks (attack type: SQL injection). The ICO later investigated and, in 2016, issued the Internet Service Provider (ISP) with a penalty of £400,000, the largest fine to date at that time, due to data losses and poor security measures (Information Commissioner's Office, 2016). Such stories continue to emerge, most recently, Carphone Warehouse were served the fine of, again, £400,000 due to "serious failure plac[ing] … over three million customers and 1,000 employees" at risk; where, a staggering "18,000 [records of] customers, historical payment and card details" were compromised (Information Commissioner's Office, 2018a).

Although the above-mentioned respondent feels companies should be "more heavily fined". Under previous legislation[69] (Data Protection Act 1998, 2005), larger fines were less likely to occur. The Information Commissioner's Office (ICO) were given permission by the UK government to serve fines up to the value of £500,000 for contraventions (The Stationery Office Limited, 2010; Information Commissioner's Office, 2015). Since, the ICO have fined Facebook and Equifax £500,000 each, the maximum set fine under the previous Data Protection Act. Facebook were fined for their role in the Cambridge Analytica scandal and Equifax for their failing to protect customers information in a cyber-attack (Information Commissioner's Office, 2018b, 2018e).

However, Information Commissioner Denham (2017) states that serving organisations with fines is last case scenario, where "guiding, advising and educating" is always primary. Denham (2017) continues with how the ICO "have always preferred the carrot to the stick", as can be identified with official statistics; where, in 2016/17 there were "17,300 cases" of which "16 of them resulted in fines for the organisations

[69] Now replaced by the Data Protection Act 2018

concerned". Yet, under new European regulatory powers General Data Protection Regulation (GDPR), fines authorised could be much larger than sums seen so far (Council Regulation (EU) 2016/679, 2016).

The GDPR, came into force on 25 May 2018, enforcing a two-tier sanction data privacy regulation, where the most serious contraventions are subject to fines up to the value of €20 million, or "up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher" (Council Regulation (EU) 2016/679, 2016). Proportionally, breaches of less serious nature are subject to fines of up to "€10 million, or "up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher" (Council Regulation (EU) 2016/679, 2016). Contraventions are measured to assess data security and protection where, considerations such as: data processing; quality; storage; transmission; disclosure; destruction; alteration and loss are all deliberated before serving fines under the new regulation. The GDPR places more control and rights for users of business services and considers the need the above-mentioned respondent makes regarding responsibility, clarity and accountability. The principles for processing personal data are to ensure accuracy and relevance, lawfulness, transparency, purpose, storage, and accountability (Council of Europe, 2016). The regulation focuses more on customer rights, than ever before, with the right to be forgotten, informed and erased displacing the responsibility of implementing appropriate technical and organisation measures for the security of individuals personal information across data controllers and processors (Council of Europe, 2016).

The total sum of fines issued in the last reported year were rumoured to reach into the billions under the new regulation; however, opposition came from Information Commissioner Elizabeth Denham (2017) who noted this as "scaremongering" is "simply scale up penalties … issued under the Data Protection Act" and that sanctions will be approached with caution and proportionally. For example, the ICO acknowledge that the fine for Facebook's role in the scandal where "an estimated 87 million users" were affected and their information unwillingly shared could have been greater under the new GDPR, considering their 2018 revenue of "£10.3 billion" (Information Commissioner's Office, 2018e; Macaulay, 2018). In more recent news, Facebook reported a breach which affected "almost 50 million of its users", something that the Irish Data Commissioner are investigating to identify if there was breach of the GDPR, where the company could be fined up to 4% of its annual turnover (Irish Data Protection Commission, 2018; Lee, 2018).

Considerations are being raised of business accountability and their proficiency in the strive to combat data loss and cybercrime under the new regulation in an almost impossible state for perfect security. Forms of risk mitigation, defences and precautions can be implemented but a perfect solution and a complete lack of vulnerabilities is unrealistic.

8.10 The View of the Public: Their views and concerns?

This section focuses on Likert based responses sought from the public audience. Participants were asked to what extent they agreed or disagreed with statements, outlined below, which focus on privacy and security, their views toward their own ability to use technology as well as protect themselves and secure their data.

Ratings were conducted on a scale of strongly agree to strongly disagree. The purpose of which was to identify people’s beliefs and rationale for previous responses and claims supporting the need for continued wider education and awareness to criminal aspects of the Internet and security preventative measures. Previous research as summarised by many authors including Foddy and Foddy (1994), Salkind (2006) and Rossi, Wright and Anderson (2013), to name but a few, have shown that the mix of statement direction (i.e. positive and negative) can be used as an attempt to reduce acquiescence bias and promote cognitive responses (e.g., cause the respondent to think more about their response). Other authors, however, have summarised how changing the direction of statements can have an effect of correlation between responses and inconsistency in responses may in fact be more difficult to control between positive and negative items dependent on samples (Ibrahim, 2001; Qasem and Gul, 2014; Solís, 2015). On reflection, the statements used in this section adopt a rather positive approach; if conducting this questionnaire again, statements would include an equal mix of positively and negatively worded statements to assess the difference in validity of responses. Considering this, the responses from the sample are described below.

- *Statement 1:* You like to use and tinker with technology

Results show that 54.9 percent of participants strongly agree or agree that they like to use and tinker with technology; on the other hand, 30.4 percent neither agree nor disagree with the statement. It may be argued these are two distinct questions, i.e., their use of technology and, their like of tinkering with technology. This research looked to identify the alliance of both. With a high proportion of people expressing neutrality, it is possible to suggest that many of the respondents use technology as a means to an end and, as an everyday object.

- *Statement 2:* You are concerned about the security of your digital devices

Results show that 86.3 percent of people strongly agreed or agreed to the concerns for the security of their devices. Previously, respondents noted how security is something which people need to be made more aware of and, educated in security measures and precautions people can take towards securing their data, devices and people online.

In addition to their use of technology and security of their devices, participants were also asked statements relating to potential concerns for their privacy and security of personal information when stored with other parties. Participants were asked the following statements:

- *Statement 3:* You are concerned about your privacy
- *Statement 4:* You are concerned that your personal information is not kept secure by websites
- *Statement 5:* You are not concerned about your online personal information being kept secure by public authorities
- *Statement 6:* You avoid disclosing personal information online

84.3 percent of respondents agreed (i.e. strongly agree or agree) they were concerned about their privacy. 73.6 percent of respondents agreed toward avoiding disclosing their personal information online. However, 17.6 percent, neither agreed nor disagreed to this suggesting that some people are unaware or have no weighted opinion when it comes to the availability and use of their personally identifiable information. Further results found that 82.3 percent and 59.8 percent of respondents agreed they were concerned that their personal information is not kept secure by websites and public authorities respectively. It is interesting to note that in previous qualitative data collected from participants in this chapter there were only a handful of people who mentioned personal information data leakage and security as a concern. Much of the heavy focus was placed on the need for awareness of and education in the use of security measures and the crimes. As opposed to the concerns of the safety of their personal information in terms of organisations and businesses. Yet here, it would suggest that respondents have an underlying concern of the use and storage of their data.

- *Statement 7:* You believe the risk of becoming a victim of a digital or cyber-related crime is increasing
- *Statement 8:* You believe you are able to protect yourself sufficiently against such crimes using precautions such as anti-virus software

94 respondents (92 percent) felt that they either strongly agreed or agreed with statement seven. This may suggest a high concern for the risks and vulnerabilities of and on the Internet including criminal activities. Lastly, respondents were asked to think about whether they agreed or disagreed they were able to protect themselves sufficiently against crimes. Participants were given the suggestion of, for instance anti-virus software at minimum, there were mixed views. Just over half (54.9 percent) agreed with statement eight; 21.6 percent stated they neither agreed nor disagreed; and 20.6 percent disagreed, with 2.9 percent stating they did not know, or the statement was not applicable.

8.11 Alignment of Public Findings in this Study

The wider focus of the study and previous stakeholder groups targeted noticeably demonstrate correlations with discipline and digital forensics education, and their relevancy does not fall into question. However, the public may still seem an unusual stakeholder group. However, the public are a key stakeholder in the educational process, as mentioned in section 8.2.1. More commonly interest from the public can be associated with the wider awareness in business and normal life for example, the need for essential cyber security and digital skills. Additionally, awareness for digital forensics may be considered important particularly considering social factors which may impact peoples' views and opinion on the punishment, prosecution, and enforcement in relation to digital crimes.

The results in this chapter have placed focus on the need for greater awareness and education, particularly toward cyber security. This is extremely relevant to moves discussed in education in chapters 2 and 3, and the funding identified for greater skills in the workforce/domain. These results also demonstrate that education may need to be included at earlier stages in the UK education. For several years, the secondary school system has seen Information Communication Technological content, opposed to Computer Science and more specific identification with cyber or emerging technologies. This has seen some improvement, however, argument for more generic skills related to cyber security may be a valid argument considering the viewpoints of participants presented above. Inevitably, the lack of Computer Science and Cyber education in secondary level teaching may have previously had a underlying impact on the prior knowledge and skills of, and expectations from, applicants, individuals looking for routes to professional development, and the general awareness of the public on what such a university course offering digital forensics and/or cyber security might offer and what skills they may gain.

8.12 Summary

Drawing on results from this section it is apparent that cyber security is a concern among the participants questioned. Focus placed on the need for knowledge in the area across all generations active online. Peoples' perception of the importance of their data and devices was likely to have been heighted by more news of cyber-attacks and loss of personal information. Results depicted highlight the disparate familiarity and understanding of digital forensics. As with many discussions throughout this research much discussion is centric to aspects of cyber security. Although, as with some participants within this public study, awareness of the need for digital forensics in tackling digital crimes is crucial. Very few participants discussed digital forensics, however, the demands and resources required in tackling digital crime were mentioned by one participant who expressed concerns at the ability of professionals to keep abreast with changes and continuous demands from small and large crimes, something they were aware was unrealistic and highly challenging. Respondents within this section felt that crimes associated with children (e.g., abuse, bullying and so on), fraudulent activities, theft (including ID theft) and violence should be at the top of the list for law enforcement when tackling cyber related events. This section is not an exhaustive view of the entire population; however, it could be argued that with over 100 participants questioned a variety of viewpoints were plausible.

9. DIGITAL FORENSICS EDUCATION: UNDERSTANDING FROM MULTIPLE STAKEHOLDERS WHAT MAKES AN IDEAL PRACTITIONER

INTRODUCTION

As the computing field continues to grow and damages associated with digital crime or digitally-enabled crime are unlikely to decelerate, so the importance of digital forensic and cyber security education and training is paramount. In the last decade, provisions for education and training within these disciplines have grown substantially to help deliver qualified and experienced individuals. Throughout this study, responses from five stakeholder groups are narrated, many included have experience of training and education within the discipline or a related computing background. This chapter looks to draw on these responses further, identifying what makes an ideal digital forensic practitioner and what educational and training improvements and skills-shortages need to be addressed within the discipline considering continual challenges the discipline faces. Views throughout this thesis have been highly subjective, a trait of a more qualitative approach, where respondent bias must be considered; for example, social desirability bias in public responses and a professional's own bias (both industry and academic) via their subject expertise and experience. This chapter seeks to provide recommendations based on the findings among discussions and narratives provided throughout this thesis to tailor improvements to curriculum and the discipline of digital forensics as the technological landscape continues to grow.

9.1 Defining Digital Forensics

While several stakeholders are considered in this subject, issues described above, and recommendations below highlight how the discipline still lacks a tangible position on its own and as an academic discipline. The subject within academia is particularly ill-defined and within academia and industry alike it lacks standardisation. Furthermore, the importance of digital forensics and cyber security as distinct disciplines is unclear with a lack of unified representation where there are a variety of views on the categorisation of the two subjects due to their similarities. The lack of definition and understanding perhaps continues to prolong the lack of well-defined positioning for the topic. The literature has shown that defining its position as its own discipline has been attempted in the past, to show its paramount importance and distinct nature. However, results in this study have shown that within education its place can still be called into question. Infancy of the discipline, as well as what some have described as the inability to define the subject with a firm grounding within academic research has arguably led to its elusiveness. Moreover, the shift toward cyber security in education has also seen movement away from digital forensics or fewer digital forensic modules and may contribute to the lack of delivery of specialist topics mentioned throughout this research. Though the focus of this thesis is placed on digital forensics, it has considered cyber security and has outlined that there are differences between the two subjects, and they are not one and the same albeit they require similar attitudes, abilities and processes. Nevertheless, a variety of questions may be covered pertaining to the subject's placement, such as:

- does digital forensics sit within computer science or forensic science?
- is it its own discipline; if so, what makes it distinct and where should it be placed?
- is digital forensics a separate discipline from cyber security?
- is digital forensics a sub-discipline of cyber security?

It is argued within the literature that digital forensics is a forensic science at the top level of characterisation, however, answering these questions is still an issue today and may continue to play into the role of the subjects ill-defined nature in academia. Several interviewees also noted that the discipline must cover several sciences (e.g., computer, forensic, criminology, policing et cetera) yet, it still needs to define itself as a scholarly topic. There are thousands of academic research papers which relate to digital forensics and several conferences which are dedicated to computer forensics and security; however, it is not a traditional/historical academic discipline including a large base of long-lasting journals with high impact factors.

Heightened awareness of security flaws and data leaks have also been a testament to the public awareness of cyber security; furthermore, the number of professionals required in roles to contend with such crimes is also apparent to much younger generations seeking an engaging and fashionable occupation. As this study saw from student and public participants the idea of what peoples' views toward digital forensics for many may still be ill-defined. While the peoples' opinions within this work have presented an understanding, this work presents there are still differing views across those working within the discipline. For instance, some stakeholders believe digital forensics should be a separate course while others believe it may be one which depicts a computer science course with a few forensic modules added. These disparate and somewhat conflicting opinions add further challenge to a discipline which already suffers in being able to define itself as its own discipline. It may also be argued that, principle focus and heavy influence for cyber security initiatives may have facilitated in the disparagement toward the development of a curriculum framework for solely digital forensics. These initiatives may have helped the subject become, as many see it, a subdiscipline of cyber security. In recent frameworks, digital forensics has been highlighted as a subdiscipline of cyber security and has close ties with certifying computer science and digital forensic courses. These challenges add to the difficulties in defining what is truly required of practitioners aiming to support the ever-growing industry and what makes them operative in a largely practical and problem-solving role.

The view as to where digital forensics places itself is one of subjectivity and to determine its position fully, greater research is required to ascertain and assess views across both disciplines and a range of stakeholders, something which this thesis suggests.

9.2 Current Education, Training and Sustainability of Curricula and Frameworks

With the rise of courses offering digital forensics and/or cyber security, the lack of applied standards and review of their impact on education could arguably influence the quality of some academic courses, sometimes suspect in delivery and style. Course analysis, reviews and professional interviewees within this study have noted how current details of academic course offerings are often non-specific and do not allow, for example, an employer to identify what a student or graduate (i.e. potential employee) has learned on their degree programme. However, academics have identified that they work with industry stakeholders when outlining and delivering courses to ensure that they provide students with a balance of theory, practice and well-rounded deliverable skills. While reviewing courses offering digital forensics, evidence of this was not found. For example, collaborators and external influencers were not mentioned, nor the process towards defining and curating curriculum and structure for courses, these were ill-defined. While it is the researcher’s own experience that can corroborate the partnership with external stakeholders in the structure and delivery of programmes and that of academics questioned in this study, there still lacks clarity.

While clarity is an issue, this must be balanced with objectiveness, flexibility and the capability for a course to, as discussed by academics, target a range of different needs from relevant business types and procedures. While balancing subjects and skills sought after within industry must take precedence in design of a course, this study suggests that course or programme outlines need to provide more precision and deliver in-depth content structure, aims and deliverables to enable individuals to make informed decisions. Decisions not only for students regarding their studies but for employability, in a time where the workforce sees numerous skills shortages. Among current UK courses there is a lack of openly available programme specifications which may provide clarity of course coverage. This is an improvement suggested to universities and training courses, not only in the UK. Furthermore, such documentation and clear outlines of specific content would allow for objective and reflective analysis of courses worldwide to distinguish if, and how, programmes can achieve the overall aim to deliver effective digital forensic skilled practitioners and/or graduates based on current and developing needs.

This study has further demonstrated the lack of clarity among courses which exist in the UK, at least by naming convention and module descriptors, for there is ostensibly an oversight of critical and developing specialist areas of digital forensics in course structures found openly online; for example, topics paramount to current digital and cyber investigations including, mobile and live data forensic analysis. While these were identified by some academics and graduates, there were problems which they pose technically for academia and by way of resourcing, key contributors to their limited inclusivity. This proposes issues for industry stakeholders in the effectiveness of a graduate straight out of university, as highlighted by few stakeholders in this research. Though it is apparent programmes, based upon course analysis, are focusing on topics which both digital forensic and cyber security establishments require from graduates, for example: networking and operating/file systems as well as the most fundamental components of computing and forensic science related to digital devices. Knowledge including how digital devices work, how they store information and what as well as how data can be recovered and techniques of analysis. Yet, what is still not clear are the depths to which these courses are successfully achieving competent graduates/practitioners within the discipline.

9.2.1 Development of a Tool for Scenario Creation

An issue which resonated with academics and participants with experience providing or attending training courses were the delivery of real-life practical teaching and learning situations. This study has highlighted how stakeholders such as, students, graduates and professionals feel there needs to be more practical learning and experience-based learning. This study has suggested the discipline could learn from academic disciplines with similar practical requirements in more experience-based teachings. Where, these suggestions could explore and have the potential to improve current issues which focus on issues such as, resourcing and the sharing of knowledge.

The use of technology to do this could be vital to the growth of the practical nature of digital forensics education, particularly with the delivery of a tool to create and/or share scenario content. Across academia and training there will be an abundance of course materials, no one programme is the same and with this come a range of scenarios built for learning, teaching and assessment. However, it is often not the case that these are widely shared or reflective of the tasks a digital forensic practitioner may experience. This study suggests a tool developed to facilitate, curate and share forensic images would be an asset to the discipline for educational and training programmes alike, considering features which address known issues within academia such as, delivering sets of images from a range of operating systems with evidence and noise through to documenting and cataloguing larger image sets for use in teaching practices. Although, the researcher acknowledges that there may be issues centric to getting such a system up and running efficiently and effectively within the academic community. The idea of a tool to facilitate scenario development is discussed below.

9.2.1.1 Argument for a Tool to Facilitate the Development, Curation and Sharing of Scenarios and Datasets

There have been several attempts to develop an automated tool used to create typical user behaviours with the output generated being an image file for educators and trainers to give to students to analyse. Examples include, Forensig2, ForGe and EviPlant (Moch and Freiling, 2009; Visti, 2013; Scanlon, Du and Lillis, 2017). Each tool is distinct and have paved the way so far and have provided a glimpse of hope for reducing the demands of creating materials within education. While neither is a fully automated tool for scenario creation this leaves academics and trainers producing and setting up machines themselves. They have to think of a realistic scenario (often changing the content to something which is not illicit e.g., replacing images with permitted ones), plant evidence on the device (this involves a number of methods/processes, data and time), make a bit-for-bit copy of the machine to provide a file for students to analyse, and then create a bank of questions and/or specific assessment tasks. This is a time-consuming duty from which several challenges arise in ensuring students are assessed and taught with a real-life digital forensics approach. The requirement for academics (for task creation) and students (for evaluation) to think like a criminal, albeit ethically, is a challenge. The forever-developing nature of criminal activities and the notion of being ‘one step behind’ adds challenges to the development of original and ‘clean’ cases which are realistic and up-to-date.

Academic respondents of this study have noted their own experiences of curating datasets as a large task, which is resource intensive and time intensive in order to develop new assessable content. The author of this thesis therefore suggests that there is a need for further collaboration within academia and industry, and a tool which can be used to fulfil these tasks. The tool should consider sharing mechanisms as well as the development of a range of images (operating/file systems and types of crime/data) as well as the need for necessary documentation.

This research highlights specifications which may be considered, but is not restricted to, based on the researchers own ideas and experiences:

- the ability to create disk images of multiple operating systems of larger sizes;
- tasks to plant and conceal evidence on disk images over a specified time period, where automated scripts are used to plant noise such as, online browsing, document creation and storage in order to increase the mass of data available and provide a realistic image;
- an environment as well as automated tasks which support a range of actions such as, deleting files, file manipulation, registry manipulation, network traffic, encryption, controlled cyber-attacks, malware, partitioning and more;
- documentation to log where all evidence to the scenario can be found (e.g. an instructor's handbook and solutions to guide educators and trainers);
- documentation which outlines a series of targets and goals, assessment questions and instructions (e.g. a student handbook, assessment or case study);
- a sharing platform used across academia and training establishments – the platform should allow academics/trainers to share their existing datasets for use on their own courses:
    - the ability to upload and store existing datasets;
    - the ability to either create or download datasets;
    - storage of datasets by categorisation (e.g. scenario, type of crime and evidential data);
    - a review system where several academics review each uploaded dataset (akin to academic paper peer-reviews) – this can be tested in class (greater risk if fails) or reviewed by a single academic or professional to check suitability and sustainability;
- the system should have a user login approach and should consider the criteria for members to add to and use the system and be a part of the solution.

Above are just some examples of what should be considered for such a tool. While these ideas are based on the ideas and experiences of the author of this work, additional work should take these ideals assessing among practitioners (educators, trainers, and professionals alike) their feasibility. Further to this, sustainability, privacy, and intellectual property rights will have to be considered. The curation, and sharing, of datasets is a hurdle which many academics come across in their delivery of courses where it is believed many may be reluctant to share their datasets due to concerns of property rights.

9.2.1.2 Feasibility of a Tools to Facilitate Scenario Creation

While a tool is suggested, this study further considers the viability of such a project which may be infeasible. For example, a tool of this nature used to enhance the educational process would have to be collaborative. This is something which stakeholders in this study note is still an issue within the discipline and needs to be addressed to ensure effective practitioners within the community. Furthermore, the scale of the tool to become successful may introduce its own unique challenges; where examples include:

- who can curate, amend, change, and delete datasets?
- who has access to uploads and can download the datasets (e.g. what is the criteria to be part of the initiative)?
- where are datasets stored and who owns them?
- who is the administrator and owner of the platform and what are their responsibilities?
- how can the platform be a success and does there need to be an authority involved?
- how to ensure all scenarios and datasets include the necessary information (e.g. are they peer-reviewed or tested on pilot student groups across numerous institutions before they are deemed a success)?
- how to ensure collaboration to deliver efficient learning situations and address specific skills/competences is the main aim?
- who accepts responsibility and accountability of damages or loss?

These are just some of the questions such an endeavour may pose, and it may well be argued that without a governing body or university provider to take responsibility for hosting of this type of platform, this specification and effort may be unsuitable in tackling current practical challenges. While this suggestion poses several thoughts and concerns, it may provide some advantages. A tool with extensive capabilities could include:

- ease of resources required for dataset creation and a speedier process due to automation;
- greater collaboration within academia, training and industry;
- share of resources and learn from each other's student experience for improved student engagement;
- improvement in the development and delivery of materials including review and sharing; and,
- a central hub for scenario and problem-based learning exercises and solutions.

9.2.2 Digital Forensic Curriculum and Frameworks: Linking Essentials, Demands and Skills Shortages

This study suggests areas which serve digital forensics and, where competence levels need to be identified including practices and development to address skills-shortages and expectations, as highlighted in Figure 9.1. This figure does not consider practitioner soft-skills though some have previously been discussed in chapter 7.

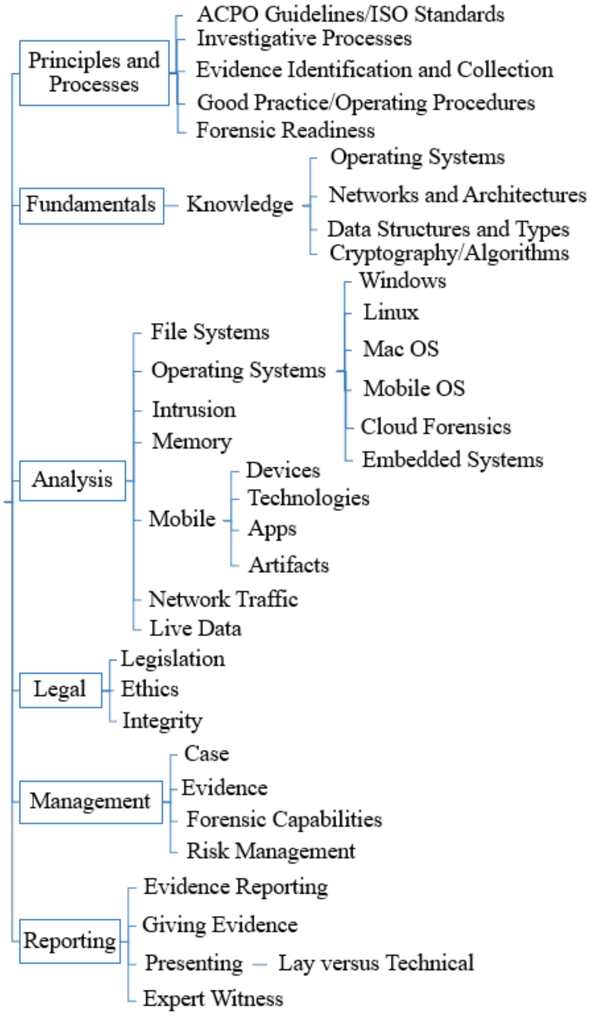


Figure 9.1 – Specialisms and Expectations mentioned by Participants of this Study

Figure 9.1 depicts six areas where technical competence have been identified from stakeholder responses, as well as current course offerings and research within the discipline. Topics are suggestive of the minimum detail of content which should be included in current digital forensic curriculums and course descriptors:

- **Principles and Processes** – Practitioners, investigative or otherwise should be aware of guidelines which support the discipline as well as standard operating procedures and good practice. Often faced with a range of digital evidence and devices they must be competent to handle a variety of investigations while ensuring integrity and preservation of data where possible. As digital forensics involves a more proactive approach through live investigations and sometimes destructive methods, practitioners must be effective and aware of a range of methodologies, concepts and procedures that may play a role in discovery and analysis. Yet, they must be aware of fundamental processes to digital forensic investigations. Courses should outline how principles and procedures are included in a curriculum, how they are assessed and how they are applied in practice to technical aspects of digital forensics.

- **Fundamentals** – While the role of a practitioner often leads to push-button forensics, they need to possess an abundance of skills which allow them to understand how digital devices are structured, how data is stored and how data can be accessed and recovered. To do this, individuals must have a relevant background of computing and competences gained in areas such as, programming/ scripting/software development, databases, networks, operating systems and file structures. Courses should include elements of computer science; however, the applicability should be wide ranging and linking with digital forensics. For example, topics such as operating systems and file structures should link with practical investigations considering forensic focus and need for Mac, Windows and Linux forensics. Skills and competences should be gained not only as generic computing knowledge but applied to in-depth understanding of how for example files can be carved from multiple systems.
- **Analysis** – There are an abundance of topics essential to a digital forensic practitioners' toolbox, however, Figure 9.1 depicts several key topics with regards to the technical and operational digital forensics analysis. While there are several courses available (education and training), the aim of these should be to encourage individuals with an analytical mindset and technical know-how, producing skilled professionals capable of more than push-button forensics. These include knowledge and awareness, skills and competences and technical skills in areas such as: mobile, network and live data forensics along with traditional computer-based forensics. Analysis includes, but is not limited to areas such as, file systems, disk data structures, file carving, registry files, deleted files, temporary files, browser data, databases, cloud analysis, smart device analysis and more. In summary, the ability to extract data from, and analyse, a diverse range of devices and data. While these topics are broad collaboration with academia and industry should identify skills, which are pertinent to the industry to deliver well-educated persons. They must have the basic understanding of recovery and analysis for a variety of technologies and data and be able to use a range of tools and techniques during an investigatory process. Courses should look to include more developing and emerging technologies in course content, beyond the once traditional computer forensics.
- **Legal** – Integrity and continuity are key components of a practitioner's abilities. They must be able to demonstrate their own integrity and reliability within an investigation while also adhering to principles and procedures, demonstrating competence and considering legalities and ethics. This is not restricted to law and policing and must consider corporate forensics and discovery and a duty to include a range of policies, regulations and laws.
- **Management** – Management refers in this case to a range of policies and regulations as well as skills and people. A digital forensic practitioner's role includes both systems and people within any

investigation. An individual must be able to manage a case, manage a substantial amount of evidence and a high workload and, will have to consider other people in the process (e.g., managers, officers, investigators, criminals, victims, jurors and so on). While a digital forensic practitioner may not encounter all people within a crime, consideration toward people skills are important especially in aspects of reporting and delivery. Courses should include relevant and applicable practical scenarios which develop these skills including group work and people skills development.

- **Reporting** – Reporting and presenting evidence is crucial to any investigation and as a digital forensic practitioner these skills are wide ranging. For example, they include demonstrable skills in witness statements and report writing where structure, language, accuracy and fact are crucial. Furthermore, reporting includes the ability to present one’s findings in a comprehensible yet technical manner clearly and concisely (i.e., both a layperson and technically educated individual should be able to understand). Giving evidence may not always be necessary, however, these skills are paramount also to explaining situations. Courses should include a variety of practical scenarios where individuals can demonstrate these skills, beyond course essays and small-scale practical solutions.

While recent workforce frameworks and certification processes centred on cyber security (with digital forensics as a specialism) have since been devised, there are similarities which may support these findings (Sobusiak-Fischanaller and Vandermeer, no date; Joint Task Force on Cybersecurity Education, 2017; NCSC, 2017b; Newhouse *et al.*, 2017). For example, the Joint Task Force on Cybersecurity Education (2017, pp. 26–27) highlight many of these topics as essential ingredients within an education, including the need for mobile forensics which this research has highlighted as a potential missing component among course analysis in the UK. Furthermore, the European Training Competency Framework (Sobusiak-Fischanaller and Vandermeer, no date) has highlighted that live data forensics along with programming, databases and networking skills are all essential to the ingredients which make an effective practitioner. In fact, Sobusiak-Fischanaller and Vandermeer (no date) demonstrate live data forensics to be an expert level ingredient to the mix required of a digital forensic investigator or examiner. Less emphasis is placed on people, soft or management skills, where reporting could be considered as an investigative technique by these authors. In addition, US works such as those by Newhouse *et al.* (2017) identify to much higher in-depth degree the skills and abilities such practitioners require and verify the essential nature of topics mentioned above with the overall aim being the ability and competence to collect, process, preserve, analyse, present and report digital evidence.

Though, the author of this research suggests caution is applied when implementing and using such frameworks or standards, particularly in a continually developing discipline which is known for its current reactive approach. Considerations towards how these guidelines are designed, as well as assessing involvement and motivations of these projects, who founded and funds each set of guidelines and any accrediting bodies should be repeatedly questioned, along with their reliability and relevance to the current situation. This has been supported by stakeholders in this study whose views on whether example frameworks could be effective in education were variable depending on the target group, where many interviewees noted that you must question how they are devised and their agenda. People noted that without these frameworks being supported at national levels (e.g. governing body of department) then the success of a framework would be infeasible. While others noted there needs to be a level of flexibility in such standards adopted to ensure that courses and content could be as diverse and informative as possible. Caution must also be placed on the longevity of these initiatives. In most cases, validity of these documentations for competences and skills will withstand technological advancements and criminality for a few years. Vandermeer (2018) supports this highlighting how an initiative of cybercrime certification will only last approximately three to five years before competences, skills and requirements would have to be re-addressed.

What is interesting is there is no set of standards or framework which is adopted within the discipline by all where this may demonstrate issues of reluctancy or caution. A European Parliament published resolution on the fight against cybercrime issued half way through this thesis still states that “currently no EU standards for training and certification exist; acknowledge[ing] that future trends in cybercrime require an increasing level of expertise from practitioners” (European Parliament, 2017, n. 71). This study has looked at US standards and UK certifications introduced in the same year, alongside the European Training Competency Framework aimed at skills for tackling cybercrime. Discussion here focused on the similarities of these frameworks to findings within this study where specific topics and skills were mentioned and attributed to the discipline. While these new efforts highlight some of the highly developing specialisms with several challenges within digital forensics (e.g., mobile, cloud live forensics), these are highlighted to be missing within several educational programmes. Based on observations by professionals these are also skills-shortages seen among graduates. This study suggests that current digital forensic programmes should consider developments which can be made to curriculums to include more investigatory technical competence for mobile, live and cloud-based using theory-practice links in both education and training situations.

9.3 Issues with Appreciation, Applicability and Contextualisation

This study has not only seen issues with collaboration within the discipline. Responses from stakeholders in this study have identified issues with unrealistic expectations, contextualisation and applicability on behalf of learners. For example, academics noted having issues with meeting and managing expectations of both students and professionals, in the latter case in relation to prospective employees who lack awareness and contextualisation.

Over focusing on theoretical knowledge linked with what some noted and perceived to be a lack of basic skills was expressed; however, these often symbolised an inability to contextualise and apply learning to practice due to a lack of experience. One professional indicated the view and the need of more practice and applicability as well as problem-solving skills shown in a graduate stating “a great 'single thing' that impressed in university, means nothing if I'm not convinced that you can apply it or replicate it in another area”. This correlates with issues focused on in chapter 6 where graduates highlighted the need for more practice yet, understood the need for theoretical and fundamental understandings of computing as well as forensics and were reflective of their inability to recognise what subjects, skills and knowledge would be important within a role in digital forensics. While appreciation for awareness and learning has been demonstrated by several stakeholders, almost on reflection, contextualisation and applicability are seemingly troubling issues within the educational discipline prior to employment.

Professionals have identified how graduates lack specific skillsets, and some have identified similarly to academics and graduates the experiences with students who are unable to answer basic questions or carry out simple, yet essentials tasks, and lack an awareness of underpinning knowledge. This is interesting and can be linked to a multitude of issues, including: management of expectations and career aspirations, lack of practical and real-life scenarios and situational learning environments, and the lack of successful collaboration between industry and academia and lack of experience, which often links with the causality dilemma of the chicken and the egg. Responses suggest that much of an alumni’s career progression in this field, on reflection, is down to their own experiences and transition of self-directed learning in a highly advancing field. Additionally, their education is a stable and fundamental underpinning to their initial learning and knowledge of the subject. Responses infer the need for continued motivation and attitudinal skills to identify how, as a practitioner, you are always learning and there is the necessity to embrace change.

Some interviewees, in the research presented, vocalised experience in presenting masterclasses to students noting their surprise when they would often be talking about tools or basic concepts and find students seemed worryingly unaware. This research further demonstrated this idea in chapter six where students were able to pinpoint important topics similar to professional expectations. Although, they were not always able to recognise the importance of softer-skills and those relating to investigative and management skills. In some cases, this could be drawn upon as being related to academic presentation and the management of perceptions and expectations. Graduates reflected how they were often unaware of, or unable to identify, how subjects, skills or tasks associated with real-life were relevant until applying concepts on-the-job.

This is not solely a problem for digital forensics, where authors such as Furnell and Kaspersky (2014) have highlighted how cyber security education also requires a balance between theory and practice and likewise must include the most basic of core knowledge. Kaspersky (Furnell and Kaspersky, 2014, p. 132) states that knowledge and practical skills in cyber security are both important:

> "[c]ore knowledge is necessary since having good basics is the reason why a security professional can go the extra mile and tackle novel problems with novel solutions. Nevertheless, without close links to practical problems or scenarios, students may finish their studies without being ready to face well-established problems and address them by means of well-established solutions."

Basic core knowledge for digital forensic graduates was a key issue stressed among professionals and graduates in this study where an individual's ability and motivation to self-learn when faced with fresh challenges was an important attribute of a digital forensics' practitioner. Thus, education in digital forensics should aim to deliver graduates with a strong background as well as sound knowledge and skills which have been acquired through several years of education to deliver an individual who may be more apt to explore, learn and research into new scenarios, challenges and adapt to evolving technological changes.

Though contextualisation and applicability are highlighted by this research as an issue with students and are an area where improvements should be made. Students and graduates should be able to place emphasis on attributes such as specific technical and non-technical skill sets they have acquired on their course and how to handle a career interview. Inability to do so, i.e., contextualise their learning with real-life scenarios and to apply learning to practice, can cause considerable problems in gaining valuable work experience and gaining employment. These issues are experienced today, and while it is recognised there is some collaboration among industry and academia, it is suggested that only with improved collaboration can these issues be tackled. In this instance, improvements may include academics working with employers to discover what issues they found with graduates when focusing specifically on contextualisation and applicability of learning with practice and the transition from education to the profession, focusing on the results. Looking to identify ways which academics can harness these issues and manage the student's expectations or improve their self-analytical skills and self-directed and reflective learning. The value of these is significantly important to the success of a graduate as a practitioner and their ability to master a technical subject.

Authors such as Van Merriënboer & Paas (2003, cited in Könings, Brand-Gruwel and Merriënboer, 2005, p. 647) stress that in order to promote active knowledge, the acquisition of competences and skills to solve real-world problems and, develop critical thinking and higher order thinking skills[70] that a learning environment or task must be "complex, realistic and challenging to elicit an active and constructive learning process". Education, while it may be contextual, a key concept of teaching is to transfer and to promote learning of knowledge and skills and, may arguably include the facilitation of students understanding and contextualisation of the field of digital forensics, its practices and, to develop cognitive independence, logical and critical thinking, reasoning and application (Angelopoulou and Vidalis, 2015; Govan, 2016; Knox *et al.*, 2018). Part of this, in a largely practical discipline like digital forensics where in-depth practice and experience are hard to come by, is about facilitating students' in their ability to contextualise their learning, be active and engage while applying their learning to real-world examples in order to achieve a concrete, effective and quality learning experience. Although, it is not solely learning strategies, aims or environments which are used to motivate student learning. Authors such as Drange, Irons and Drange (2017) discuss how creativity is also imperative Their own ability to identify and reflect upon their own knowledge gain and learning skills is as important (De Corte, 1990 cited in Könings, Brand-Gruwel and Merriënboer, 2005, p. 648).

Authors such as Govan (2016, pp. 58–60) discuss how these skills are important for digital forensic graduates in order to possess deep knowledge where "higher order learning and the development of soft enabling attributes" such as, articulation are fundamental pillars to the specialist career. Govan (2016, p. 60) along with other authors such as, Garrison, (1997) and Halpern and Hakel (2003) identify that the goal of higher education is to deliver independent and self-directed learners; where, "self-directed learning provides graduates with a collection of transferable skills, attributes and strategies which encourage graduates to become lifelong learners". Many authors have noted the fruitfulness of self-directed and independent learning appearing across degree studies and adult education, most notably Malcolm Knowles (1975).

Grow (1991, p. 129) categorises four stages of self-directed learning through the Staged Self-Directed Learning (SSDL) model explaining how an educator's purpose is to encourage learners to work from a dependent learner (e.g., someone who requests direction from others) through to self-direction (e.g., someone who can set their own goals and needs no direction from a facilitator). Kandiko and Mawer (2013, p. 51) acknowledge there is the need for independent learning in academia with a balance of "sufficient guidance to facilitate learning". Academics within digital forensics have contributed works which show

[70] Higher order thinking skills: Bloom's Taxonomy.

efforts towards improving learning processes and self-directed learning while moving aside traditional teacher-centric methods for those which deliver engaging and active learning situations including, Game Based Learning and Problem Based Learning (Pan, Schwartz and Mishra, 2015; Irons and Thomas, 2016). Furthermore, Knörl *et al.* (2015, p. 315) highlight that self-directed learning lends itself well to educating students in Software Engineering, identifying how a student's own understanding of self-directed learning also plays a central role in their ability, curiosities and motivations for learning. Though there are several attributes and challenges of self-directed and independent learning which are highlighted by the authors such as Knörl *et al.* (2015, p. 315), depicted in Figure 9.2.

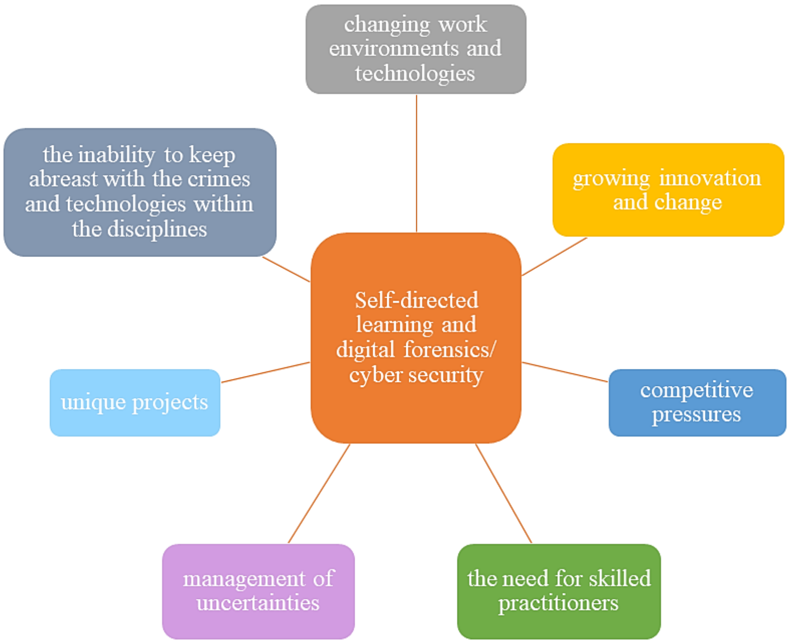

changing work environments and technologies
the inability to keep abreast with the crimes and technologies within the disciplines
growing innovation and change
Self-directed learning and digital forensics/ cyber security
unique projects
competitive pressures
management of uncertainties
the need for skilled practitioners

Figure 9.2 – Self-directed learning applied to digital forensics/cyber security

These are comparable with several issues found within the disciplines of digital forensics and cyber security. For example, challenges with the "brisk pace … of the changing Software Engineering field" (Knörl *et al.*, 2015, p. 315) can be likened to the continuous fast-paced changes and developments with digital and cyber investigations. Similarly, the pressure of the working environment, technologies and managerial and unique projects are all an insurmountable aspect within digital forensics.

Tiwana (2002 cited in Ginty and Boland, 2016, p. 10) identifies "knowledge as a fluid mix of framed experience, value, contextual information, expert insight and grounded intuition that provides an environment and framework for evaluation and incorporating new experiences and information." It is suggested that digital forensics education must consider how to address these issues and provide improved framed experiences and perceived value as well as promote and facilitate students' skills of reflection and their awareness and ability to apply and put into context their learning in relation to the real-world. While there have been improvements and advances in the delivery and design of digital forensics education, few authors within digital forensics education research have identified the issues students have when applying, reflecting, and contextualising their learning for employment. This research has demonstrated that these are issues which resonated among stakeholder narratives in this study, and these may be the causal effect of the lack of experience and expert insight to the digital forensic industry which students obtain.

9.4 A Practical Discipline: How can it learn from others?

Professional and graduate responses highlighted the need for more scenario, problem-based and practical learning with less theory. Although, theory and experience were analysed and believed to be important by both students and graduates; where, half the professionals questioned felt experience was just as important as qualifications and training. Graduates were able to reflect on the theory learned and establish theory-practice links when on-the-job. Thus, results suggest that some academic programmes and training provisions offer, at some level, suitable learning given discussions with graduates and professionals. However, also highlighted are the challenges and demands of an ever-growing profession which in some respects do not align with what professionals expect or need (e.g. practical skills and technical skills to reduce the skills-shortages in areas of analysis and softer skills). While graduates have identified experience of practice and theory intertwined, there is still more requirement for practice within the academic discipline for effective theory-practice links. While placement opportunities are offered at most universities, academics have found problems in collaborations, where students have not taken the opportunity and where professional responses infer that students/graduates do not have enough practical application or applied experience.

Academics have also noted there to be a range of different needs from related businesses. Expressing how they must provide students with diverse knowledge, skills, and activities for real-life work, aligning to more than one sector or business for employability. For example, results in this study (chapters 6 and 7) have highlighted how students need to be open to both public and corporate forensics and security, where digital forensics is no longer aimed in totality at policing and must consider client handling and management for corporate investigations. This suggests the skill of adaptability of graduates to adjust to “different environmental conditions and situational contexts” as similarly outlined by the (Joint Task Force on Cybersecurity Education, 2017, p. 79) for cyber security professionals. This study suggests that the discipline could learn from other disciplines as well as the organisation of graduate programmes offered by businesses after degree completion.

Previously discussed in this thesis were the links which may be made between the practical nature or medicine and that of digital forensics; where, medical education sees students take a hands-on approach through compulsory placements to provide individuals with not only real-life experience but allow them to ponder their career decisions and learn valued skills. Working in situational settings allows for deeper understanding and application of theoretical content and provides enhanced learning experiences; these are issues currently observed in digital forensics (discussed throughout chapters 5-7). Similarly, businesses often provide specialist graduate career programmes, particularly seen in the IT sector for fresh graduates from university. These are training schemes used to introduce graduates into a business, often lasting a couple of years. In this time individuals are offered opportunities to experience several areas of the business, rotating through general or specialist areas before making a choice on their career direction. Apprenticeship schemes are also career opportunities which offer real-life experience on-the-job, plus education, and have seen an increase in adoption in the last few years. This thesis suggests digital forensics education could adopt similar approaches where programmes look to adopt the benefit through provision which deliver education with mandatory industrial integrated placements.

Arguably, these could provide students with an essential ingredient: experience; however, this type of approach would require better collaboration between industry and academia, a theme evident through responses from both graduates and professionals. Previous challenges highlighted between placement opportunities in education and industry have included the limited possibilities within digital forensics, as well as issues with the profession being highly security conscientious. Other issues may include the time and effort on behalf of an employer for the supervision of individuals on placement in what is a profession already suffering from high and sensitive workloads. Yet, similar hurdles can be identified in many disciplines which offer placements particularly those which require discretion, confidentiality, protection and integrity. Additionally, professionals are suggesting the need for more practical experience including placement opportunities and recognised collaboration as a key component to the solution; however, students and academics alike are finding they must set their sights on other computing roles within industry to ensure placement opportunities are provided.

This thesis argues that educational initiatives could combine the benefits of these initiatives and include mandatory industrial placements across a range of businesses providing a rotation and focus on specialist areas within digital forensics and/or cyber security (e.g. computer forensics, mobile device forensics, network security or forensics, e-Discovery, corporate investigations, information security forensics, system administration et cetera). While these would pose challenges, and there is no authority to make this mandatory among known digital forensic providers (educational and professional) this could address key issues such as the siloed nature which digital forensics struggles and improve on collaboration experienced throughout the discipline so far. These initiatives could be used to promote benefits to both industry and education where issues could be addressed including:

- challenges of changing technologies and crime;
- educational challenges in providing real-life scenarios and practical assessments;
- challenges and awareness of career opportunities and expectations;
- the need for and balance of education, training and experience;
- limited skills and skill shortages of current workforces and expanding amounts of evidence;
- the continued need for practitioners with the necessary knowledge and skills to competently carry out the work of a digital forensic practitioner;
- issues found among graduates relating to applicability of their learning, contextualisation or appreciation;
- coordination and collaboration among industry, academia, and training partners.

While benefits may be achieved by such initiatives there is the danger that learning could be reduced to competency-based training as address in the work by Harreveld and Singh (2009, pp. 99–100), who look at secondary education and discuss how to achieve contextualised learning, partnerships are essential to "scaffold [a] students' learning and … develop real-world curriculum from within [] new learning spaces". Future works should consider the feasibility of these initiatives and look at educational transformations in this field while acknowledging there is a need to address the siloed nature within digital forensics.

9.5 Digital Forensic Roadmaps to Implementing Effective Education

This section takes into consideration the analysis of this study and provides several roadmaps to implementing effective digital forensic education and contextualises the roles of key stakeholders documented in this study.

This study discovered several challenges which digital forensics education and training face. These range from problems with resourcing through to the challenges that come from a discipline which is fast paced, ever-changing and highly practical. This study identifies that there are often issues with application and contextualisation on behalf of students and graduates which must be addressed by educators. However, in most cases, it is not until a graduate is employed and applying their knowledge that they master both application and contextualisation.

Additionally, issues lie within education, which for professionals and employers become stumbling blocks, particularly identifying the content taught on a course and the knowledge and skills obtained on behalf of the students. While some courses provide this information, it is largely broad and brief. For instance, a course may recognise it includes content such as mobile forensics in a digital forensic module. As an outsider or professional it may be hard to decipher the duration of this content and/or the depth of knowledge acquired. For example, is it just two-weeks work of mobile forensic content at a theoretical level, or is it a whole semester in which students learn the concepts, principles, and theory, and apply these in practical ways either manually or using industry tools? Furthermore, the extent of the practicality of courses is often unaddressed in course briefings. While these issues have been demonstrated as hurdles for outsiders such as employers and professionals to utilise in decision-making processes around graduates, they are also a hurdle for applicants, students, and graduates alike. In addition, academics must manage expectations and facilitate context for a range of stakeholder groups.

These issues have been discussed in chapters above. From these results in chapters 5 through to 8 a set of roadmaps have been devised which concentrate on the key stakeholder groups. These roadmaps use data collected and analysed in this study to demonstrate some of the key aspects, knowledge, skills, and attributes which should be accounted for within digital forensics education. The roadmaps are based on the narratives told by academics, graduates, students, and professionals.

This research contributes to knowledge and identifies five roadmaps. One for each key stakeholder group presented in this study, namely:

- academics/educators,
- applicants,
- students,
- graduates, and
- professionals/employers.

9.5.1 Concept, Development, and Creation of the Roadmaps

This section discusses the overall concept of the roadmaps and identifies the aims of each roadmap for the different stakeholder groups. Furthermore, the development and creation of the roadmaps are highlighted to identify how the various findings within this research are being utilised and how they provide a new contribution. To assess the roadmaps they will be exposed to validation in the form of expert commentary drawn from relevant stakeholders. Analysis of those reviews are also presented in this section.

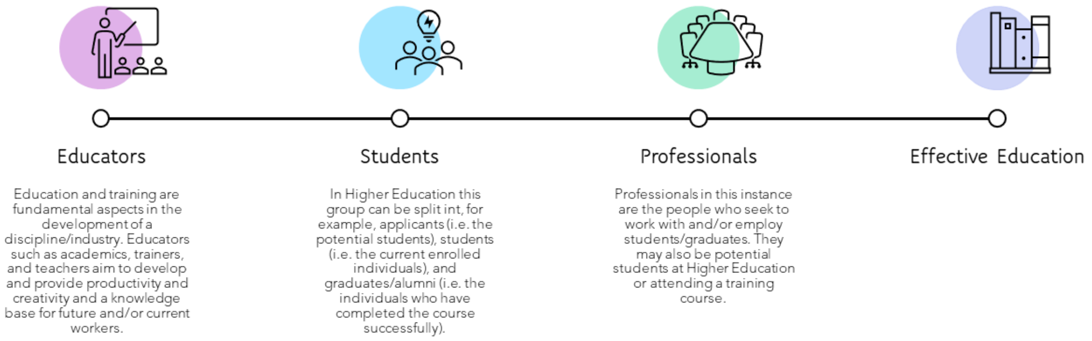
9.5.1.1 Concept

This research contributes five roadmaps that are proposed to facilitate the implementation of an effective education in digital forensics. Each roadmap considers a stakeholder group that each play a different role within digital forensics education.

The stakeholder groups were not only decided upon due to the coverage within the previous chapters of this study, but due to their involvement in the educational process. Figure 9.3 depicts the stakeholder groups. Each was decided upon due to the role they play or should be expected to play in the education process. For example:

- Educators (academics/trainers) are essential for the development and delivery of a knowledge base that an individual can apply to a profession.
- Students (applicants, current, alumni) are necessary not only for a program to be delivered, but also to reflect upon the delivery and application of the content during and after a course has been successfully completed. They are essential for the growth of any workforce.
- Professionals (individuals, employers) are required to facilitate the applicability of a course and its theory-practice links to the everyday tasks of a range of different roles within an industry/discipline. They are also valuable in understanding the current challenges and improvements required among education and training offerings.

These are just some examples of how different stakeholder groups link to the effectiveness of a course and the individuals produced and demonstrate that cooperation is key between each group to successfully reflect upon the effectiveness of education and/or training.



Education and training are fundamental aspects in the development of a discipline/industry. Educators such as academics, trainers, and teachers aim to develop and provide productivity and creativity and a knowledge base for future and/or current workers.

In Higher Education this group can be split int, for example, applicants (i.e. the potential students), students (i.e. the current enrolled individuals), and graduates/alumni (i.e. the individuals who have completed the course successfully).

Professionals in this instance are the people who seek to work with and/or employ students/graduates. They may also be potential students at Higher Education or attending a training course.

Figure 9.3 – Stakeholder Groups Considered for Digital Forensic Education Roadmaps

Public stakeholders, while a group considered within this research, were removed during the development of the roadmap at this stage, as the researcher felt the applicability of such a roadmap would be less valuable in achieving an effective digital forensics education within higher education. However, inclusion of the stakeholder group is potential for further research.

When drawing the stakeholder groups together, and the proposed roadmaps, a wider collaborative effort is required to achieve an effective education. The roadmaps are therefore devised to facilitate aspects of education/program development, learning or employability.

The aim of each roadmap is outlined below:

- Educators: *to facilitate the development and delivery of a course in digital forensics.*
- Applicants: *to identify questions, tasks and concepts applicants should consider when looking for, and choosing a course in digital forensics.*
- Students: *to facilitate the decisions students make, and how they apply their learning to gain employment.*
- Graduates: *to facilitate their learning process and employability chances by identifying topics, attributes and skills required.*
- Professionals/Employers: *to facilitate the employment of graduates by outlining concepts, shortfalls and expectations which can be achieved.*

9.5.1.2 Development and Creation of the Roadmaps

The roadmaps are created based on the key themes discussed throughout the chapters of this thesis i.e., from the analysis of views and experiences discussed with participants of this study. These are found in chapters 5 through to 7. As previously noted, discussions with interviewees led to the analysis of a range of responses from different stakeholder groups and individuals with differing lengths of experience. Themes were identified within and across the key stakeholder groups. Various key themes were outlined in chapters 6 and 7; these have been the key source of reflection on which the roadmaps have been established. The proposed roadmaps are therefore developed in the context of relevant stakeholder opinions and experience within digital forensics education and industry and relevant journeys. However, it was identified that the roadmaps, for purposes of rigour, should be evaluated by experts[71] within digital forensics.

9.5.1.3 The Initial Roadmaps

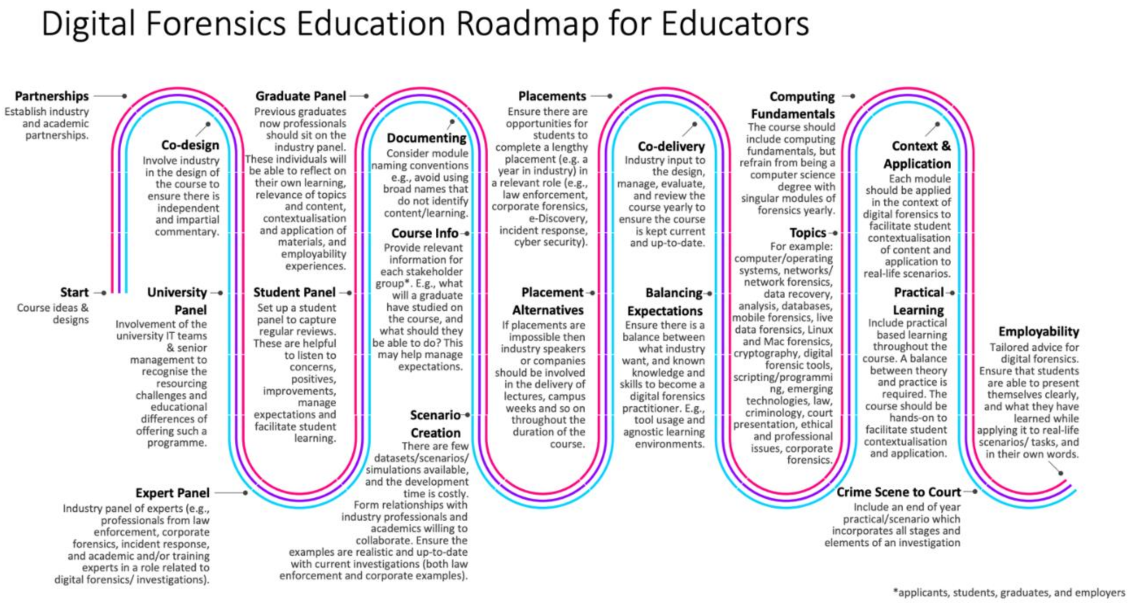
Each roadmap considers phases which were deemed by the researcher to be most relevant to the potential group of individuals and their potential journey toward an effective education. Each phase reflects on the issues and key themes drawn in previous chapters and consults how each roadmap may affect the other. For example, the advice given to educators should also compliment the information applicants, students,

[71] Experts in this case were people who had academic and/or industry experience.

graduates, and professionals are presented with and vice versa to facilitate improved collaboration, management of expectation and improved application to the industry roles.

This section demonstrates the roadmaps in their initial form i.e., before expert commentary/review. The final versions of the roadmaps can be seen in Appendix G – G.3.

Educators



Digital Forensics Education Roadmap for Educators

Start
Course ideas & designs

Partnerships
Establish industry and academic partnerships.

Co-design
Involve industry in the design of the course to ensure there is independent and impartial commentary.

University Panel
Involvement of the university IT teams & senior management to recognise the resourcing challenges and educational differences of offering such a programme.

Expert Panel
Industry panel of experts (e.g., professionals from law enforcement, corporate forensics, incident response, and academic and/or training experts in a role related to digital forensics/ investigations).

Student Panel
Set up a student panel to capture regular reviews. These are helpful to listen to concerns, positives, improvements, manage expectations and facilitate student learning.

Graduate Panel
Previous graduates now professionals should sit on the industry panel. These individuals will be able to reflect on their own learning, relevance of topics and content, contextualisation and application of materials, and employability experiences.

Documenting
Consider module naming conventions e.g., avoid using broad names that do not identify content/learning.

Course Info
Provide relevant information for each stakeholder group*. E.g., what will a graduate have studied on the course, and what should they be able to do? This may help manage expectations.

Scenario Creation
There are few datasets/scenarios/ simulations available, and the development time is costly. Form relationships with industry professionals and academics willing to collaborate. Ensure the examples are realistic and up-to-date with current investigations (both law enforcement and corporate examples).

Placement Alternatives
If placements are impossible then industry speakers or companies should be involved in the delivery of lectures, campus weeks and so on throughout the duration of the course.

Placements
Ensure there are opportunities for students to complete a lengthy placement (e.g. a year in industry) in a relevant role (e.g., law enforcement, corporate forensics, e-Discovery, incident response, cyber security).

Co-delivery
Industry input to the design, manage, evaluate, and review the course yearly to ensure the course is kept current and up-to-date.

Balancing Expectations
Ensure there is a balance between what industry want, and known knowledge and skills to become a digital forensics practitioner. E.g., tool usage and agnostic learning environments.

Topics
For example: computer/operating systems, networks/ network forensics, data recovery, analysis, databases, mobile forensics, live data forensics, Linux and Mac forensics, cryptography, digital forensic tools, scripting/programming, emerging technologies, law, criminology, court presentation, ethical and professional issues, corporate forensics.

Computing Fundamentals
The course should include computing fundamentals, but refrain from being a computer science degree with singular modules of forensics yearly.

Context & Application
Each module should be applied in the context of digital forensics to facilitate student contextualisation of content and application to real-life scenarios.

Practical Learning
Include practical based learning throughout the course. A balance between theory and practice is required. The course should be hands-on to facilitate student contextualisation and application.

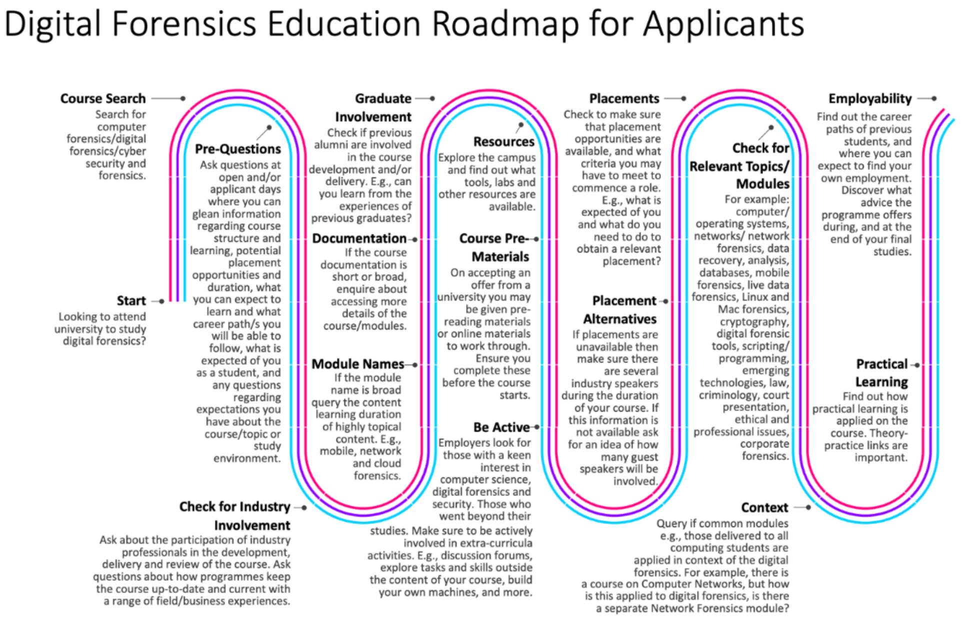
Crime Scene to Court
Include an end of year practical/scenario which incorporates all stages and elements of an investigation

Employability
Tailored advice for digital forensics. Ensure that students are able to present themselves clearly, and what they have learned while applying it to real-life scenarios/ tasks, and in their own words.

*applicants, students, graduates, and employers

Figure 9.4 – Digital Forensic Education Roadmap for Educators (Initial Version)

Applicants



Digital Forensics Education Roadmap for Applicants

Start
Looking to attend university to study digital forensics?

Course Search
Search for computer forensics/digital forensics/cyber security and forensics.

Pre-Questions
Ask questions at open and/or applicant days where you can glean information regarding course structure and learning, potential placement opportunities and duration, what you can expect to learn and what career path/s you will be able to follow, what is expected of you as a student, and any questions regarding expectations you have about the course/topic or study environment.

Check for Industry Involvement
Ask about the participation of industry professionals in the development, delivery and review of the course. Ask questions about how programmes keep the course up-to-date and current with a range of field/business experiences.

Module Names
If the module name is broad query the content learning duration of highly topical content. E.g., mobile, network and cloud forensics.

Documentation
If the course documentation is short or broad, enquire about accessing more details of the course/modules.

Graduate Involvement
Check if previous alumni are involved in the course development and/or delivery. E.g., can you learn from the experiences of previous graduates?

Resources
Explore the campus and find out what tools, labs and other resources are available.

Course Pre-Materials
On accepting an offer from a university you may be given pre-reading materials or online materials to work through. Ensure you complete these before the course starts.

Be Active
Employers look for those with a keen interest in computer science, digital forensics and security. Those who went beyond their studies. Make sure to be actively involved in extra-curricula activities. E.g., discussion forums, explore tasks and skills outside the content of your course, build your own machines, and more.

Placement Alternatives
If placements are unavailable then make sure there are several industry speakers during the duration of your course. If this information is not available ask for an idea of how many guest speakers will be involved.

Placements
Check to make sure that placement opportunities are available, and what criteria you may have to meet to commence a role. E.g., what is expected of you and what do you need to do to obtain a relevant placement?

Check for Relevant Topics/ Modules
For example: computer/ operating systems, networks/ network forensics, data recovery, analysis, databases, mobile forensics, live data forensics, Linux and Mac forensics, cryptography, digital forensic tools, scripting/ programming, emerging technologies, law, criminology, court presentation, ethical and professional issues, corporate forensics.

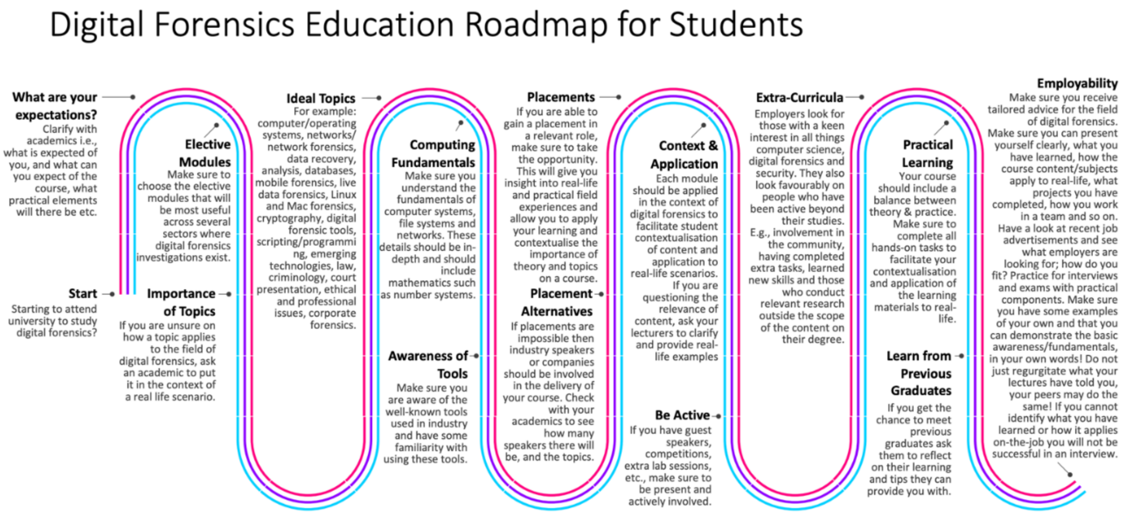
Context
Query if common modules e.g., those delivered to all computing students are applied in context of the digital forensics. For example, there is a course on Computer Networks, but how is this applied to digital forensics, is there a separate Network Forensics module?

Practical Learning
Find out how practical learning is applied on the course. Theory-practice links are important.

Employability
Find out the career paths of previous students, and where you can expect to find your own employment. Discover what advice the programme offers during, and at the end of your final studies.

Figure 9.5 – Digital Forensic Education Roadmap for Applicants (Initial Version)

Students



Digital Forensics Education Roadmap for Students

What are your expectations? Clarify with academics i.e., what is expected of you, and what can you expect of the course, what practical elements will there be etc.

Start Starting to attend university to study digital forensics?

Elective Modules Make sure to choose the elective modules that will be most useful across several sectors where digital forensics investigations exist.

Importance of Topics If you are unsure on how a topic applies to the field of digital forensics, ask an academic to put it in the context of a real life scenario.

Ideal Topics For example: computer/operating systems, networks/network forensics, data recovery, analysis, databases, mobile forensics, live data forensics, Linux and Mac forensics, cryptography, digital forensic tools, scripting/programming, emerging technologies, law, criminology, court presentation, ethical and professional issues, corporate forensics.

Computing Fundamentals Make sure you understand the fundamentals of computer systems, file systems and networks. These details should be in-depth and should include mathematics such as number systems.

Awareness of Tools Make sure you are aware of the well-known tools used in industry and have some familiarity with using these tools.

Placements If you are able to gain a placement in a relevant role, make sure to take the opportunity. This will give you insight into real-life and practical field experiences and allow you to apply your learning and contextualise the importance of theory and topics on a course.

Placement Alternatives If placements are impossible then industry speakers or companies should be involved in the delivery of your course. Check with your academics to see how many speakers there will be, and the topics.

Context & Application Each module should be applied in the context of digital forensics to facilitate student contextualisation of content and application to real-life scenarios. If you are questioning the relevance of content, ask your lecturers to clarify and provide real-life examples

Be Active If you have guest speakers, competitions, extra lab sessions, etc., make sure to be present and actively involved.

Extra-Curricula Employers look for those with a keen interest in all things computer science, digital forensics and security. They also look favourably on people who have been active beyond their studies. E.g., involvement in the community, having completed extra tasks, learned new skills and those who conduct relevant research outside the scope of the content on their degree.

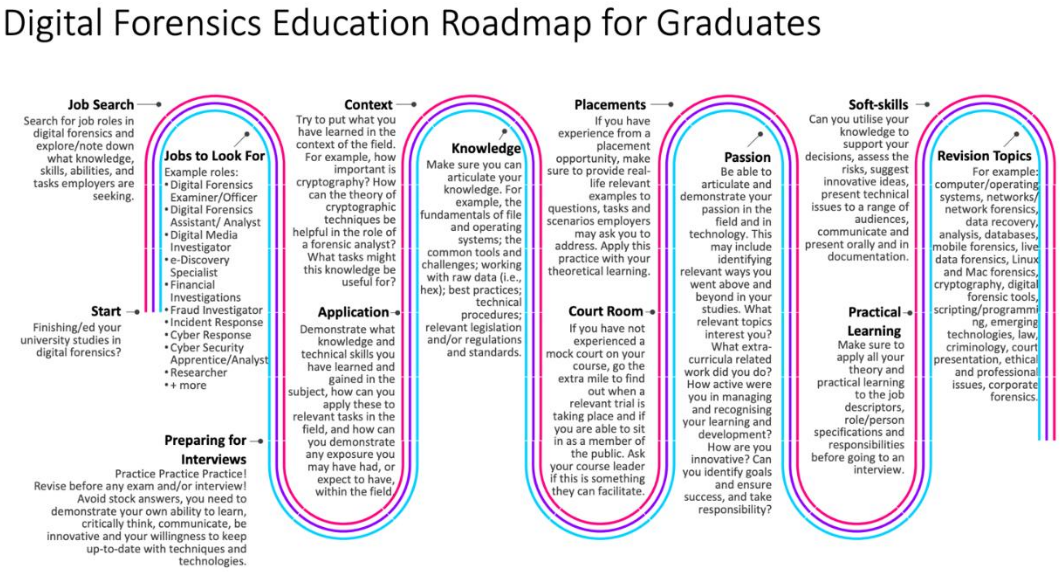
Practical Learning Your course should include a balance between theory & practice. Make sure to complete all hands-on tasks to facilitate your contextualisation and application of the learning materials to real-life.

Learn from Previous Graduates If you get the chance to meet previous graduates ask them to reflect on their learning and tips they can provide you with.

Employability Make sure you receive tailored advice for the field of digital forensics. Make sure you can present yourself clearly, what you have learned, how the course content/subjects apply to real-life, what projects you have completed, how you work in a team and so on. Have a look at recent job advertisements and see what employers are looking for; how do you fit? Practice for interviews and exams with practical components. Make sure you have some examples of your own and that you can demonstrate the basic awareness/fundamentals, in your own words! Do not just regurgitate what your lectures have told you, your peers may do the same! If you cannot identify what you have learned or how it applies on-the-job you will not be successful in an interview.

Figure 9.6 – Digital Forensic Education Roadmap for Students (Initial Version)

Graduates/Alumni



Digital Forensics Education Roadmap for Graduates

Job Search Search for job roles in digital forensics and explore/note down what knowledge, skills, abilities, and tasks employers are seeking.

Start Finishing/ed your university studies in digital forensics?

Jobs to Look For Example roles:

- Digital Forensics Examiner/Officer
- Digital Forensics Assistant/ Analyst
- Digital Media Investigator
- e-Discovery Specialist
- Financial Investigations
- Fraud Investigator
- Incident Response
- Cyber Response
- Cyber Security Apprentice/Analyst
- Researcher
- + more

Preparing for Interviews Practice Practice Practice! Revise before any exam and/or interview! Avoid stock answers, you need to demonstrate your own ability to learn, critically think, communicate, be innovative and your willingness to keep up-to-date with techniques and technologies.

Context Try to put what you have learned in the context of the field. For example, how important is cryptography? How can the theory of cryptographic techniques be helpful in the role of a forensic analyst? What tasks might this knowledge be useful for?

Application Demonstrate what knowledge and technical skills you have learned and gained in the subject, how can you apply these to relevant tasks in the field, and how can you demonstrate any exposure you may have had, or expect to have, within the field.

Knowledge Make sure you can articulate your knowledge. For example, the fundamentals of file and operating systems; the common tools and challenges; working with raw data (i.e., hex); best practices; technical procedures; relevant legislation and/or regulations and standards.

Placements If you have experience from a placement opportunity, make sure to provide real-life relevant examples to questions, tasks and scenarios employers may ask you to address. Apply this practice with your theoretical learning.

Court Room If you have not experienced a mock court on your course, go the extra mile to find out when a relevant trial is taking place and if you are able to sit in as a member of the public. Ask your course leader if this is something they can facilitate.

Passion Be able to articulate and demonstrate your passion in the field and in technology. This may include identifying relevant ways you went above and beyond in your studies. What relevant topics interest you? What extra-curricula related work did you do? How active were you in managing and recognising your learning and development? How are you innovative? Can you identify goals and ensure success, and take responsibility?

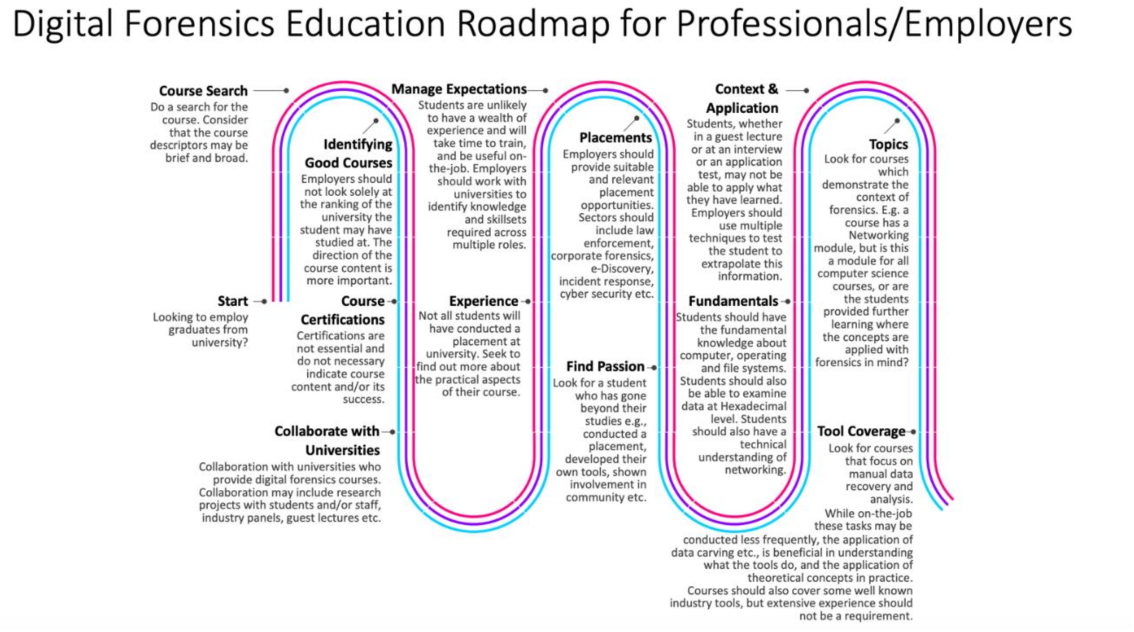
Soft-skills Can you utilise your knowledge to support your decisions, assess the risks, suggest innovative ideas, present technical issues to a range of audiences, communicate and present orally and in documentation.

Practical Learning Make sure to apply all your theory and practical learning to the job descriptors, role/person specifications and responsibilities before going to an interview.

Revision Topics For example: computer/operating systems, networks/network forensics, data recovery, analysis, databases, mobile forensics, live data forensics, Linux and Mac forensics, cryptography, digital forensic tools, scripting/programming, emerging technologies, law, criminology, court presentation, ethical and professional issues, corporate forensics.

Figure 9.7 – Digital Forensic Education Roadmap for Graduates (Initial Version)

Professionals/Employers



Digital Forensics Education Roadmap for Professionals/Employers

Start
Looking to employ graduates from university?

Course Search
Do a search for the course. Consider that the course descriptors may be brief and broad.

Identifying Good Courses
Employers should not look solely at the ranking of the university the student may have studied at. The direction of the course content is more important.

Course Certifications
Certifications are not essential and do not necessary indicate course content and/or its success.

Collaborate with Universities
Collaboration with universities who provide digital forensics courses. Collaboration may include research projects with students and/or staff, industry panels, guest lectures etc.

Manage Expectations
Students are unlikely to have a wealth of experience and will take time to train, and be useful on-the-job. Employers should work with universities to identify knowledge and skillsets required across multiple roles.

Experience
Not all students will have conducted a placement at university. Seek to find out more about the practical aspects of their course.

Placements
Employers should provide suitable and relevant placement opportunities. Sectors should include law enforcement, corporate forensics, e-Discovery, incident response, cyber security etc.

Find Passion
Look for a student who has gone beyond their studies e.g., conducted a placement, developed their own tools, shown involvement in community etc.

Context & Application
Students, whether in a guest lecture or at an interview or an application test, may not be able to apply what they have learned. Employers should use multiple techniques to test the student to extrapolate this information.

Fundamentals
Students should have the fundamental knowledge about computer, operating and file systems. Students should also be able to examine data at Hexadecimal level. Students should also have a technical understanding of networking.

Topics
Look for courses which demonstrate the context of forensics. E.g. a course has a Networking module, but is this a module for all computer science courses, or are the students provided further learning where the concepts are applied with forensics in mind?

Tool Coverage
Look for courses that focus on manual data recovery and analysis. While on-the-job these tasks may be conducted less frequently, the application of data carving etc., is beneficial in understanding what the tools do, and the application of theoretical concepts in practice. Courses should also cover some well known industry tools, but extensive experience should not be a requirement.

Figure 9.8 – Digital Forensic Education Roadmap for Professionals/Employers (Initial Version)

9.5.2 Review of the Digital Forensic Roadmaps

To validate these roadmaps, four independent professionals provided expert commentary. The respondents included educators across two countries, each with seven or more years' experience and professional practice in industry and/or education. Participants included:

- educators with experience in computer science and cyber security/digital forensics,
- educators with both industry, academic and training experience in digital forensics.

Participants were provided with a consent form, information about the research, and a copy of each roadmap. The researcher asked each of the participants to consider the roadmaps before an interview, or feedback was provided via email where individuals were extremely busy. Participants were given at least two days to review the materials before any commentary was provided.

Participants were asked four key questions which are outlined, and the responses discussed below:

1. What do you think about the roadmaps and the applicability to their stakeholder groups?
2. Do you think the roadmaps facilitate a student's journey from applicant to the profession, given your experience?
3. Please describe any enhancements you consider feasible for the roadmaps.
4. Do you have any additional feedback or comments?

9.5.2.1 Applicability of the Roadmaps

All professionals (n=4) responded that they felt the roadmaps were applicable to the stakeholder groups, and that they would be useful within education.

Quote from Transcript A:

> "Yes. I think that the roadmaps are useful for digital forensics education. They highlight key considerations for program developers as well as the students throughout the studies. As an academic myself I particularly think that the roadmaps for applicants, students, and graduates pin-point items we as academics try to deliver ultimately managing their expectations of a course and by extension, the discipline."

Quote from Transcript B:

> "Yes, I think the roadmaps are applicable, and very helpful for the stakeholders."

Quote from Transcript C:

> "I think they are. … I think the biggest problem from my point of view is it is problematic for employers to know what they want, and students do not know what is expected of them. It is not until you are experienced and doing the job that you know what is expected of you, and the skills that are required."

Quote from Transcript D:

> "Yes I do. Some parts of the "Educators" might be a bit resource demanding, but nevertheless I think they should all be there - something to stretch for."

9.5.2.2 Facilitation from Study to Profession

All four participants agreed that the roadmaps could facilitate the student journey, identifying that the roadmaps attract people to think outside of the curriculum or program and think more long term about their progression and careers. For example, snippets from the transcripts of Participants A, B and C:

Quote from Participant A:

> "I think it is possible that these roadmaps allow the students to think about what they are looking for and learning and facilitates them in identifying specific questions they should ask themselves about their progression and involvement in a course. I think the three key

> things across the roadmaps are the ability to manage expectations, apply their learning, and be able to contextualise what they have learned with real-life examples and scenarios."

Quote from Participant B:

> "The roadmaps facilitate the perfect student from applicant to become a professional. However, most students do not do all these assessments of the courses before attending a program. Your roadmap will really help students."

Quote from Participant C:

> "I think the roadmap is really good overall. I think it touches on a lot of topics here. … For example, what you say here about passion and you need to work on things outside the studies and do things outside the curricula is quite good. … at the same time, a lot of the education in this field is done in a lot of sectors that do not have experience on-the-job. My studies were by people who did not have the practical experience, and they had been taught by people who also did not have the practical real-world experience. The problems given to us were theoretical and they were problems you do not necessarily encounter in the real world, so they were not close to what you do when you start working in the field. … What I would really like here is more collaboration with Police and others alike who have the necessary experience from real-world examples."

However, participant C highlights issues that have been mentioned previously in this study and contribute toward content in the roadmaps such as practical scenarios, experience (e.g. placements), the involvement of several stakeholders including industry and so. The participant highlights a problem which was also documented over ten years ago in the literature (seen in chapter 2), and that is the lack of professionals who have moved to education and who can provide education that is true to real life examples. Again, pinpointing that the discipline requires greater collaboration between its stakeholders to deliver effective education and that there is a requirement for academia to employ "people from public and private sectors to have teachers and trainers who are more experience and who can deliver scenarios that are applicable to the real-world tasks and cases".

Participant D also agrees that the roadmaps are suitable, however, they identify that their own students may not follow such a pathway. This highlights that depending on the student audience, the pathway may differ.

Quote from Participant D:

> "I do not think our students follow such a roadmap, not even close. But they are already employed and have a more relaxed approach to doing our courses. However, "ordinary" students might be following a similar roadmap."

9.5.2.3 Enhancements

Participants were asked to consider enhancements that would be of benefit to the delivery of the roadmaps. Key themes that were drawn from these responses included the re-arrangement of topics such as placement opportunities and their alternatives through to comments about the focus of the knowledge about common industry tools and open source counterparts. These themes are discussed below and addressed in the final versions of the roadmaps presented in chapter 10 and Appendix G.

Placement Opportunities

Each diagram considers placement opportunities and the potential for alternatives. Ideally students would benefit from placements on all courses, sometimes this may require a placement outside of digital forensics and in the wider IT sector. This was mentioned by academics in previous interviews and the necessity to manage the student expectations on the type of placements they can obtain in a relevant role. Both Participant B and D felt that the order of the placement alternatives and placement opportunities should be swapped within the diagrams.

Quote from Participant B:

> "I think when the educator creates a study addressing the placements opportunities should be performed before identifying the placement alternatives (more logical order), and placements programs at companies should be selected based on how well they follow good practice. However, this requires a perfect cooperation with the industry."

Panels

The research included several panels in the educator roadmap, something which is not unfamiliar across academia are the idea of students and industry panels. In the educator roadmap a graduate panel was also included to facilitate the reflection of the course materials and progression, and to look toward how to address the issues of awareness, contextualisation, and applicability. However, Participant B felt there were too many panels and that an overarching approval process/management and one that included all industry, students, and graduates together.

Quote from Participant B:

> "I also think there were to many panels assessing the course. Would it be better having two? One for the University management/board approval process, and one for the input from industry, students, and graduated together? In addition course surveys is excellent for detecting strengths and weaknesses of a particular course."

Participant D also mentioned the graduate panel presented in the education roadmap in their comments. The participant highlights concerns about identifying what is essential to the fundamental knowledge rather than quantity. A valid reflection which also demonstrates crossovers with the tools as an element of study.

Quote from Participant D:

> "Graduate Panel - I see this could be a good idea, but how would you make sure such a panel does not focus too much on quantity and not quality. E.g. in the police they would prefer to hire a person who could reduce their back-log rather than doing a thorough job which takes a lot of time. So, in terms of employability, they would say "Learn how to use Encase and XRY, because that is what is needed"."

This point was not addressed by the research as it is considered a wider problem where taking onboard the feedback from relevant stakeholder groups must be actioned with caution and consider the developments within digital forensics education over the last decade, and focus on the fundamental knowledge and skills an individual will need to acquire to fit into any number of roles related to the field of digital forensics.

Commercial Tools vs Open Source

In addition to the idea of learning how to use standard industry tools mentioned above, participants B and D continue to highlight this within the roadmaps. Initially the roadmaps identified that students and graduates should have an awareness of well-known industry tools and some familiarity with using them. This point was conceived based on discussions with previous industry participants who acknowledged that over the years education has focused on the use of open source tools. The participants acknowledged this is great as students get to learn what the tools do and the application of theoretical concepts. However, while they agreed education offerings should not train the students how to use the tools, they should at least have a familiarity with what well-known tools are available, what they do, and how to use them even at a very basic level. Previous participants were more concerned with the fundamental knowledge such as how to interpret hexadecimal and so on using tools. This justified the need to include the tools within the roadmaps as something to deliver or something to look out for and learn, however, from comments from participants B and D, the roadmaps seemingly suggest that it is only the well-known tools that should be addressed within educational programmes.

Quote from Participant B:

> "I do not think programs need to teach the commercial forensic suites. Post-graduates may attend commercial training courses after finishing the program instead. I think open source tools is better to learn digital forensics. When applying for a position where a specific tool is used as the main tool, they should consider attending training for this tool."

Quote from Participant D:

> "Awareness of tools - Why is this important? Should the education be tool independent? Maybe this is more important the day you start looking for a job, as within the industry there might be a variety of tools in use. More so within LE where special developed tools are in use. I see that this is at an awareness level, but also that they should, to some extent, learn how to use these tools."
>
> "Still I do not see why education should cover well known industry tools (presuming proprietary)."

This was not what the researcher intended, and therefore the final versions of the roadmaps address the value of open source tools. It should be mentioned that both participants B and D work with open source tools as their main source of teaching and therefore there is an element of bias. However, use of open source tools in education and their value was not only mentioned by participant B and D, but previous academic respondents, industry participants, and previous literature.

Applying the Roadmaps

Participant C felt that the roadmaps were good, "have addressed quite a lot of the issues" and provided value. However, they noted that it "it is quite one thing to address it in a roadmap and address it in real-life". The participant's key points were that the wider issue of collaboration between academia and industry needed to be addressed for education to become more effective. The participant noted that there are many issues or mindsets that hinder greater collaboration though, it is the key issues the discipline must overcome. This was previously identified within this chapter by various participants across the stakeholder groups.

Increased collaboration would for example address comments made by Participant B and C regarding issues such as:

- Industry not knowing what they want or what to expect of a digital forensic practitioner.
- Students not knowing what knowledge, skills, and tasks they should expect in a digital forensic role.
- Academia hiring more public and private sector professionals who have greater experience.
- Education being able to deliver real-life cases/scenarios.
- Applying current research where it is applicable for the profession.
- Finding and achieving better practice to push the domain forward.

9.5.2.4 Additional Comments/Feedback from Expert Commentary

In addition to the discussions above, this section also highlights a short list of enhancements that could be made to the roadmaps as part of future versions/revisions of the roadmaps.

Educators

Participant A:

- Sustainability of the courses
  - the roadmap could consider refreshment of course within its cycle (e.g. how to address the re-design, re-development, and repetition of some steps)
  - considering courses which already exist and implementation of the roadmap

Participant B:

- Employability - Seems to be quite resource demanding. But I guess this could be done at the end of a programme and not after every course

Students

Based on Participant D comments:

- The researcher identifies that future revisions of student roadmaps should consider different types of students, study levels, student backgrounds, and extend to the delivery of education/training for professionals.

All Roadmaps

Participant A:

- Reduce quantity of textual content in the roadmaps

9.6 Summary

This chapter has drawn on several of the key aspects found among research conducted in this study and provided several suggestions and insight into the current state of digital forensics education. Suggestions made are considered future improvements of education within the discipline to provide effective practitioners for industry. Consideration is also given to the needs and encouragement of students to become specialised in more than one topic or task, a balance of expectations in industry and by students and to ensure the delivery of a widely educated digital forensic individual. This chapter draws together data from previous chapters and provides a cohesive output in the form of comprehensive roadmaps for key stakeholders.

10. CONCLUSION

Research conducted in this study looked to identify what is expected of a digital forensics' practitioner, what makes them ideal (e.g., work ready and the skills/knowledge they require), along with the current state of curricula on offer as well as any future educational improvements. To do this, this thesis draws together the views, opinions and experiences of 201 participants across five stakeholder groups (academics, graduates, students, professionals and the public). The subjective nature of what defines an 'effective digital forensics practitioner' was discovered through responses from the varying groups. Studies presented in this thesis have shown how the competences and skills expected of a practitioner and fundamental to digital forensics are subjective based on attributes such as experience, professional role and peoples' own experiences of education and training. However, this study has also shown there are commonalities among these views, such as subjects and skills expected of practitioners.

As a rich and distinct discipline facing several challenges professionally and within the education sector, digital forensics programmes should be designed to reflect the industry's wide encompassing values and its continual need to keep abreast with current and emerging technologies and unlawful activities. This thesis argues that this can only be accomplished within education through inclusive understanding of all stakeholder opinions, ideals and experience. The importance of these stakeholder responses is vital to understanding the current status quo of the discipline and what is essential to delivering effective practitioners. For example, professionals who experience the daily role of a digital forensics' practitioner can enhance a curriculum by identifying the most fundamental knowledge and skills required of an educated individual. Graduates provide academics and the course evaluation with insightful reflections on the positives and negatives to current curriculum structures against their new on-the-job roles, experiences and initial challenges and integration into the workplace. Furthermore, academics can provide a wealth of experience and identify challenges among educators and trainers towards managing expectations of students and industry alike, where this research acknowledges there must be balance in the breadth and depth to which stakeholder views may be applied within curriculum development and delivery.

This thesis has drawn upon these opinions and experiences to highlight some of the issues that exist today for digital forensics education and attitudinal or topical areas which need improvements; for example:

- issues with contextualisation and awareness among learners and graduates and the need for more practical experience;

- the importance of basic and fundamental knowledge and skills (e.g. basic knowledge of computers, the ability to reading/manipulating/work with hexadecimal data, basic coding skills, familiarity with industry tools);
- the significance of topics such as: Linux forensics, Linux as investigative tool, programming, networking, mobile forensics, file systems and operating systems;
- the need for practitioners with greater understanding of, for example, mobile forensics, malware analysis, live forensics and Mac forensics.

10.1 Addressing the Research Questions and Goals

This thesis focused on three original overarching research questions and several aims. This section revisits these and discusses the questions by addressing how they have been approached along with original contributions. Results throughout chapters in this work have revealed that there are several themes pertinent across stakeholders.

10.1.1 What is the current curriculum for digital forensics?

To identify the current state of digital forensics education, this research considered the development of higher education courses using existing literature, through analysis of 32 undergraduate programmes using readily available information such as course content and descriptors from UK higher education and the voices of academics. Reviewing these showed how offerings have shifted from computer forensics towards cyber security inclusive of digital forensics. Furthermore, how curricula, at the time of analysis, centred on basic computing knowledge and concepts in first-year studies. These were outlined by professionals, academics and graduates (chapters six and seven) as important knowledge for both digital forensic and cyber security practitioners and included topics such as, programming and scripting, networking, databases, computer security and computer operating and file systems as well as basic forensic knowledge and techniques. However, this thesis has shown that analysis by module naming convention and readily available course descriptors alone cannot provide a suitable level of clarity to understand what exactly is covered on a course in digital forensics. Descriptions and names are often broad and do not show what the students are being taught, this can only be grasped by access to course materials. This often meant that courses were missing topics such as mobile forensics, cloud data forensics, live data forensics, malware analysis and Mac forensics; topics which were mentioned by professionals as skills-shortages or of increased importance within the field (chapter seven). Due to the lack of clarity, the content as well as skills and abilities cannot be assessed thoroughly and goes beyond analysis within this thesis, this is considered something for future research.

Challenges relating to digital forensics education identified within the literature and by academics include staff resourcing and knowledge, technical resourcing and the lack of collaboration across industry and academia (chapters five and six). While collaboration has improved over the last decade this is something which alumni and students note needs more work to achieve efficacy in digital forensics education. Academics in chapters five and six also noted challenges of dedicated laboratories while others recognising issues still present today in the application of practical approaches to learning due to time and resource intensive scenario curation, and challenges with placement opportunities. Something which is recognised by professionals as something which the field and education need to address (chapter seven). In particular, the use and delivery of datasets which must be created and the notion of making them realistic (e.g. time settings, timelines, plots, evidence and case load). Many note current examples are outdated or do not address current and relevant issues, some of the issues include case management and workloads (e.g., number of devices, mass of data and criminal activity) due to this lengthy process and resource intensive development. There is also a limited willingness to share datasets and examples. In order to achieve this, realistic materials need to be created. For this, greater collaboration with industry is required to reproduce the systems, data and challenges they are seeing on the frontline. This thesis has suggested a tool for scenario creation noting specific functionality and the need for a system to share and facilitate with developments across educational offerings (chapter five) where more content on specialist forensics and areas such as, cryptography, malware, mobile, cloud and live data forensics and incident response should be considered for development.

10.1.2 What are the challenges and developments towards a curriculum framework reflective of industry needs?

The literature often describes the subject as a fresh interdisciplinary discipline; yet, digital forensics has existed in academia for over a decade and in industry for over three decades. Looking at digital forensics as a field and within education, the literature covered in chapter three has shown problems with defining the subject, awareness and settlement as an academic discipline. Few scientific journals have been sustainable, and publications have struggled to reach high index, citation and impact factors. Furthermore, the discipline has suffered from debates over standardisation and certification for several years where the literature reviews in this thesis have acknowledged there is a lack of formal positioning and standards within the field and attempts have often brought to attention more debates. This has often been centric to its inclusion of multifaceted disciplines such as, computer science, law, criminology and policing and forensic investigation. Supporting this, views from academics ranging from Heads of Schools and Professors to Senior Lecturers many with over 10 years' experience in academia and/or professionally in computer/digital forensics have acknowledged problems facing the position of the academic discipline including the perceived notion to satisfy all areas which the subject comprises, adding to the displacement of the field as an academic discipline.

At the beginning of this study very little work had been conducted on standards towards an effective curriculum within digital forensics. Much of the work had included course outlines of initial programmes across countries such as the US and UK as discussed in chapter two. However, new frameworks were introduced in countries such as the US and UK and in Europe to provide standardisation from national bodies, a focus of chapter three. These works have been shown to concentrate on workforce profiles and certification of undergraduate and postgraduate courses; yet, there is still no formal standardisation of education and training requirements within the discipline. Most frameworks have shaped deliverables for cyber security and documented digital forensics as a specialist area due to the close relationship of the two disciplines. Observed in chapter three are these works where common trends are discussed and used as comparison for narratives captured from various stakeholders in this study. This work is unable to review these attempts to standardise digital forensics education, or look at their effect, as they are out of scope. It is suggested that further work examine this, particularly how standardisation may help continue to shape digital forensics and cyber security as an academic challenge.

10.1.3 What makes an effective digital forensic practitioner and/or curriculum?

In a discipline which is forever growing and suffering from a range of technical advances and challenges undoubtedly there will be several skills-shortages of the current forces who are practicing digital forensics. Rapid growth of digital technologies, the vast sources of evidence, increased storage sizes and diverse formats has led to challenges within digital forensic investigations; such as lengthy backlogs and large associated costs for equipping and maintaining a forensic lab. Furthermore, challenges include the availability of forensic analysts and the relatively small budgets within law enforcement. Much of this is largely due to ubiquitous technologies such as smart devices and increased use of cloud applications and storage. Such challenges highlight the need for knowledgeable and skilled practitioners within digital forensics. Public opinions and views have shown that education and awareness are still an issue among the general populous around cyber security, digital forensics, and cybercrime. Chapter eight covered topics and crimes that participants felt law enforcement should be tackling along with how people can become better educated and concerns addressed. These highlighted how the role of digital forensic and cyber security practitioners needs to defined and highlighted for a range of stakeholders beyond professionals with knowledge of the disciplines.

Various stakeholders questioned in this study have identified skills-shortages among graduates and the industry alike and have included malware, mobile, cloud and live data forensic analysis and incident response (chapters five to seven). While topics such as operating systems, networking and programming were exhaustively found in course naming conventions and common expectations by professionals, these same professionals emphasised that some graduates lack these fundamental understanding and skills to demonstrate their learning and practical abilities. For example, chapter seven saw professionals identify skills-shortages and inexperience of graduates they had seen including examples such as, basic technical skills, general knowledge of hardware/devices, the ability to read and manipulate hexadecimal, working with offsets and tables, basic coding skills, familiarity with industry standard tools and the inability to troubleshoot from first principles. Some of these responses can be attributed to issues observed by professionals, academics, and graduates towards the inability to contextualise and apply their learning and, suggest requirements and improvements of educational offerings to manage and nurture these among students.

Yet other responses suggest there are improvements required within digital forensics education to include more relevant, challenging, and specialised subjects such as, mobile forensics. Most professionals noted their experience had led them to believe there was sufficiently a lack of practical exposure and awareness toward experience in forensic analysis, data structures and using current industry digital forensic tools, as well as a lack of awareness to the practical issues and challenges the industry are facing, seen in chapter seven. By giving voice to several stakeholders within digital forensics and those impacted by education and training for this research, their views and experiences have illustrated pertinent topics and expectations of a professional, as discussed in chapter nine.

The challenges faced by the discipline highlight the importance of stakeholder views on what should be included in digital forensics education to produce an effective workforce for digital forensics. For example, the knowledge and experience of professionals who are faced with the daily challenges of digital technologies and graduates for their reflection of educational programmes and improvements.

10.2 Limitations and Justifications

This section features the limitations of this research and proposes justifications. One limitation of this study was the number of participants. Convenience sampling was applied in this study in effort to gain access to a range of individuals across the five stakeholder groups, however, this resulted in fewer responses than anticipated. In total 201 participants are included in this research. Half of these participants are from the public while the stakeholder group with the least participants were graduates. A lack of participants is suggested due to the community being relatively small and largely founded upon a secure and protective approach in what is still an ill-defined discipline from current literature. In particular, fewer numbers for graduates and professionals may be expected in a discipline which suffers from lengthy case backlogs and lack of skilled practitioners. A range of responses from differing roles and length of experience also show that the discipline requires further collaboration among stakeholders where, this may also suggest why samples are lower than anticipated. A limitation of this study is the number of professionals/alumni who, at the time, had 2 or fewer years' experience interviewed or surveyed. While this may have its negatives such as little experience to reflect upon, those with few years' experience and an educated background may have been able to reflect upon their studies and integration into a workplace to provide insightful feedback with less difficulties. Future research should look to obtain responses from more individuals and with more experience in a role relating to digital forensics.

Questionnaires and interviews were based on calls for participants through convenience sampling where the researcher was reliant on known associates as well as the distribution of calls on social media, forums, and via emails. This research suffered from several issues when gaining access to participants. These included: public bodies who were unable to pass on questionnaires to relevant staff, no response to correspondence and small amounts of collaboration. It is suggested that different sampling methods are considered for future research and a wider national study; for example, from an institution or governing body related to digital forensics may address these issues seeking a greater number of responses and range of academic and professional views.

While gaining access and sample sizes are small for this type of research, respondents were people with a vast range of experience within industry and academia. Individuals included analysts, investigators and managers who had worked in the discipline for several years, some over ten years, through to academics who were Professors, Heads of Schools and Senior Lecturers with academic and professional practice. While each group of respondents are not an exhaustive representation of their stakeholder industry, data saturation was used to ensure findings were based on information provided by respondents portraying similar and relevant themes. Repetition of key topics, issues, observations and experiences shown across the five stakeholder groups showed opinions and experiences were similar, where data saturation was observed. Revised or new studies should look to identify expectations, skills-shortages and experiences of degree programmes and practitioners focusing on academic, graduate and employer comments and collaborations from more respondents using different sampling methods.

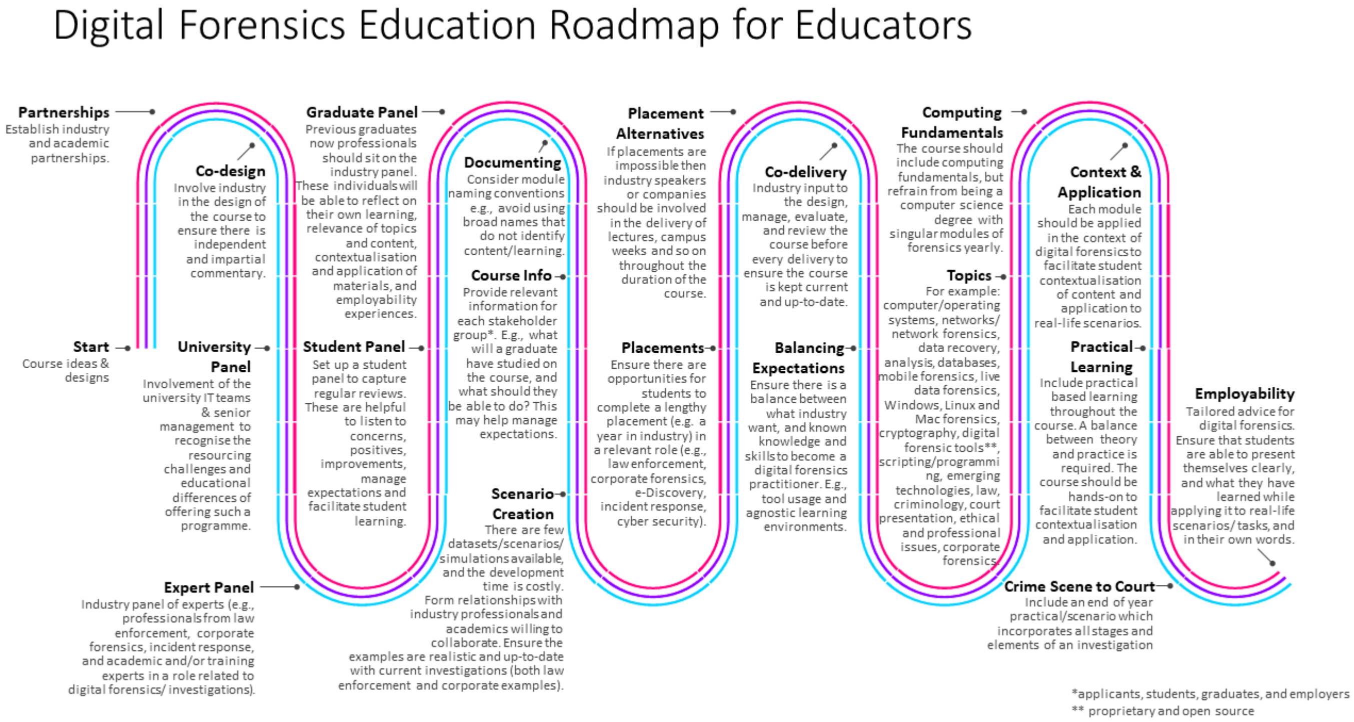
Another limitation of this thesis is the inability to examine current UK certifications and standards toward digital forensics within higher education and their effects. The certifications discussed based on available documentations were introduced in 2016/17 where, for example, few institutions have provisional or full certification (e.g., the NSCS Certification of Bachelor's Degrees in Computer Science and Digital Forensics). This meant assessing the implication and effects of these standards was infeasible within this study. A new study should consider how these standards were adopted within the curricula based on academic experiences and views of the NCSC where, the impact, if any, on course delivery, uptake of courses, through to effects on employability of graduates and what has been taught or learned should be discovered. These works were in initial stages of adoption at the end of this study and examination of their progress, implementation and impact, the researcher believes, would prove beneficial to understanding whether digital forensics continues to fulfil industry demands and whether standardisation of an ill-defined discipline is a suitable venture.

10.3 Contribution to Knowledge

This research brings together analysis of five target groups using interviews and questionnaires on aspects of digital forensics skills shortages within industry and education. Contribution has been made in the identification of higher education within the UK and its delivery from both literature review and examination of modules provided across several degree programmes. Furthermore, this thesis has pointed to the main expectations of graduates to be or become an effective digital forensic practitioner based on professional, graduate and academic opinions and experiences. To date there are limited works which have pursued these views, comparing, and contrasting the requirements and challenges the growing discipline faces. This thesis has contributed to knowledge by highlighting how courses still need to include more practical and hands-on experiences of real-life cases within both education and training; where a balance of theory and practice is required. It has also demonstrated that works toward cyber security frameworks, to some degree, align with opinions and expectations of professionals polled but addresses the need to approach standardisation with caution. This thesis has also demonstrated topics which professionals have found to be lacking in graduates or those they acknowledge as fundamental skills-shortages within the industry. This implies a greater need for collaboration among the digital forensic profession.

Finally, this thesis has provided original contribution in the form of stakeholder roadmaps. These final versions of the roadmaps are depicted below in Figure 10.1 – Figure 10.5 and can be found in Appendix G – G.3. The proposed roadmaps, discussed in chapter 9, were devised to facilitate the development and improvement of digital forensic education programs, their effectiveness, and to address the roles of stakeholder groups within the educational process. These works were derived from themes, challenges, ideas, and more presented throughout this thesis and are based on existing literature, and the views and experiences of a range of individuals and professionals across the stakeholder groups discussed throughout.

10.3.1 Digital Forensic Education Stakeholder Roadmaps



Digital Forensics Education Roadmap for Educators

Start
Course ideas & designs

Partnerships
Establish industry and academic partnerships.

Co-design
Involve industry in the design of the course to ensure there is independent and impartial commentary.

University Panel
Involvement of the university IT teams & senior management to recognise the resourcing challenges and educational differences of offering such a programme.

Expert Panel
Industry panel of experts (e.g., professionals from law enforcement, corporate forensics, incident response, and academic and/or training experts in a role related to digital forensics/ investigations).

Graduate Panel
Previous graduates now professionals should sit on the industry panel. These individuals will be able to reflect on their own learning, relevance of topics and content, contextualisation and application of materials, and employability experiences.

Student Panel
Set up a student panel to capture regular reviews. These are helpful to listen to concerns, positives, improvements, manage expectations and facilitate student learning.

Documenting
Consider module naming conventions e.g., avoid using broad names that do not identify content/learning.

Course Info
Provide relevant information for each stakeholder group*. E.g., what will a graduate have studied on the course, and what should they be able to do? This may help manage expectations.

Scenario Creation
There are few datasets/scenarios/ simulations available, and the development time is costly. Form relationships with industry professionals and academics willing to collaborate. Ensure the examples are realistic and up-to-date with current investigations (both law enforcement and corporate examples).

Placement Alternatives
If placements are impossible then industry speakers or companies should be involved in the delivery of lectures, campus weeks and so on throughout the duration of the course.

Placements
Ensure there are opportunities for students to complete a lengthy placement (e.g. a year in industry) in a relevant role (e.g., law enforcement, corporate forensics, e-Discovery, incident response, cyber security).

Co-delivery
Industry input to the design, manage, evaluate, and review the course before every delivery to ensure the course is kept current and up-to-date.

Balancing Expectations
Ensure there is a balance between what industry want, and known knowledge and skills to become a digital forensics practitioner. E.g., tool usage and agnostic learning environments.

Computing Fundamentals
The course should include computing fundamentals, but refrain from being a computer science degree with singular modules of forensics yearly.

Topics
For example: computer/operating systems, networks/ network forensics, data recovery, analysis, databases, mobile forensics, live data forensics, Windows, Linux and Mac forensics, cryptography, digital forensic tools**, scripting/programming, emerging technologies, law, criminology, court presentation, ethical and professional issues, corporate forensics.

Crime Scene to Court
Include an end of year practical/scenario which incorporates all stages and elements of an investigation

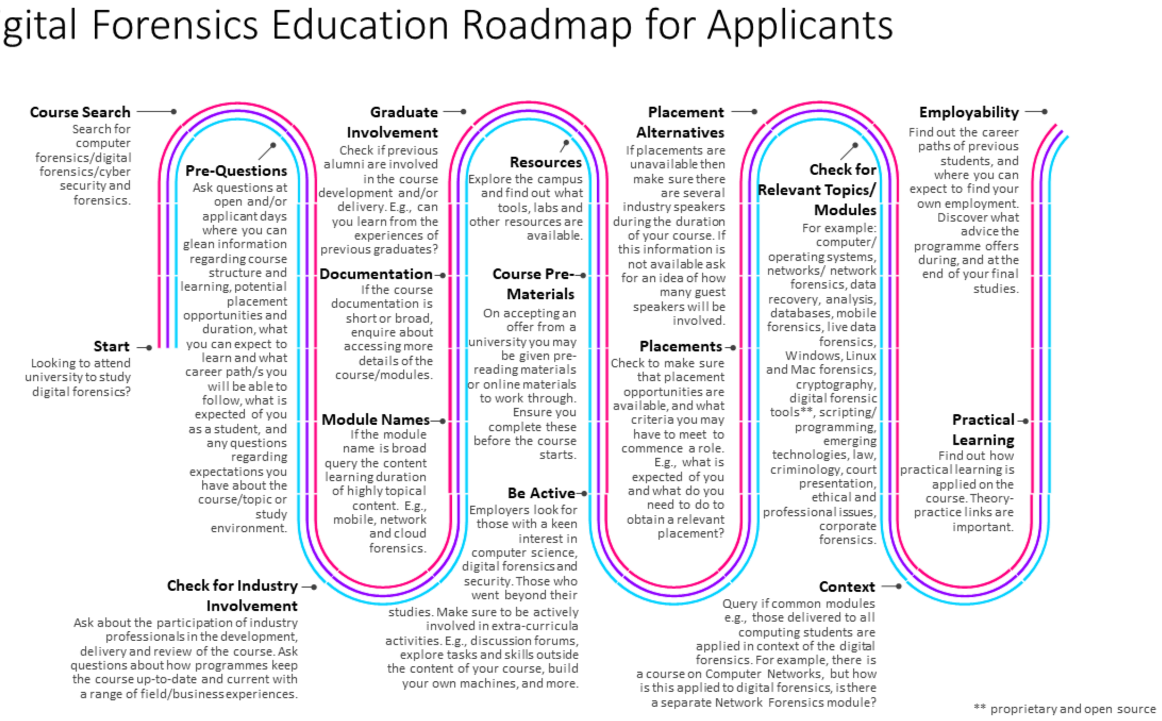
Context & Application
Each module should be applied in the context of digital forensics to facilitate student contextualisation of content and application to real-life scenarios.

Practical Learning
Include practical based learning throughout the course. A balance between theory and practice is required. The course should be hands-on to facilitate student contextualisation and application.

Employability
Tailored advice for digital forensics. Ensure that students are able to present themselves clearly, and what they have learned while applying it to real-life scenarios/ tasks, and in their own words.

*applicants, students, graduates, and employers
** proprietary and open source

Figure 10.1 – Digital Forensic Education Roadmap for Educators (Final Version)



Digital Forensics Education Roadmap for Applicants

Start
Looking to attend university to study digital forensics?

Course Search
Search for computer forensics/digital forensics/cyber security and forensics.

Pre-Questions
Ask questions at open and/or applicant days where you can glean information regarding course structure and learning, potential placement opportunities and duration, what you can expect to learn and what career path/s you will be able to follow, what is expected of you as a student, and any questions regarding expectations you have about the course/topic or study environment.

Check for Industry Involvement
Ask about the participation of industry professionals in the development, delivery and review of the course. Ask questions about how programmes keep the course up-to-date and current with a range of field/business experiences.

Graduate Involvement
Check if previous alumni are involved in the course development and/or delivery. E.g., can you learn from the experiences of previous graduates?

Documentation
If the course documentation is short or broad, enquire about accessing more details of the course/modules.

Module Names
If the module name is broad query the content learning duration of highly topical content. E.g., mobile, network and cloud forensics.

Resources
Explore the campus and find out what tools, labs and other resources are available.

Course Pre-Materials
On accepting an offer from a university you may be given pre-reading materials or online materials to work through. Ensure you complete these before the course starts.

Be Active
Employers look for those with a keen interest in computer science, digital forensics and security. Those who went beyond their studies. Make sure to be actively involved in extra-curricula activities. E.g., discussion forums, explore tasks and skills outside the content of your course, build your own machines, and more.

Placement Alternatives
If placements are unavailable then make sure there are several industry speakers during the duration of your course. If this information is not available ask for an idea of how many guest speakers will be involved.

Placements
Check to make sure that placement opportunities are available, and what criteria you may have to meet to commence a role. E.g., what is expected of you and what do you need to do to obtain a relevant placement?

Check for Relevant Topics/ Modules
For example: computer/ operating systems, networks/ network forensics, data recovery, analysis, databases, mobile forensics, live data forensics, Windows, Linux and Mac forensics, cryptography, digital forensic tools**, scripting/ programming, emerging technologies, law, criminology, court presentation, ethical and professional issues, corporate forensics.

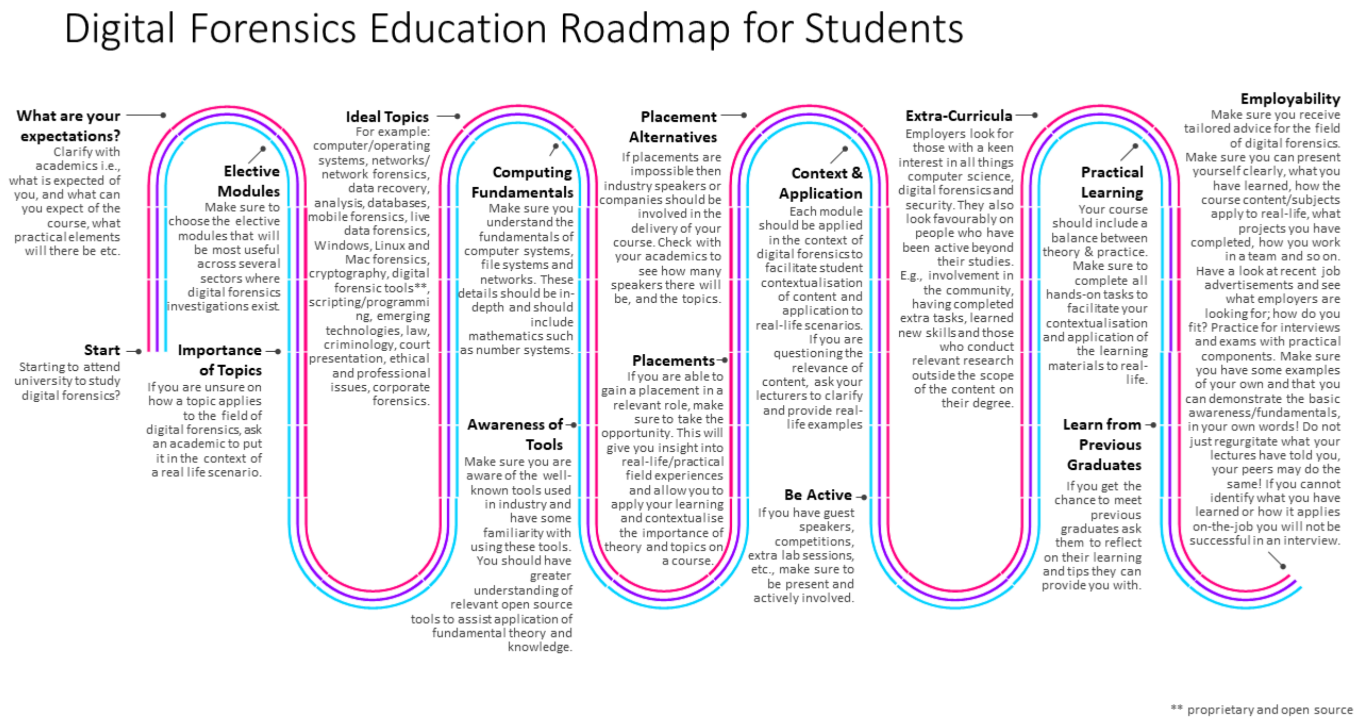
Context
Query if common modules e.g., those delivered to all computing students are applied in context of the digital forensics. For example, there is a course on Computer Networks, but how is this applied to digital forensics, is there a separate Network Forensics module?

Practical Learning
Find out how practical learning is applied on the course. Theory-practice links are important.

Employability
Find out the career paths of previous students, and where you can expect to find your own employment. Discover what advice the programme offers during, and at the end of your final studies.

** proprietary and open source

Figure 10.2 – Digital Forensic Education Roadmap for Applicants (Final Version)



Digital Forensics Education Roadmap for Students

Start Starting to attend university to study digital forensics?

What are your expectations? Clarify with academics i.e., what is expected of you, and what can you expect of the course, what practical elements will there be etc.

Elective Modules Make sure to choose the elective modules that will be most useful across several sectors where digital forensics investigations exist.

Importance of Topics If you are unsure on how a topic applies to the field of digital forensics, ask an academic to put it in the context of a real life scenario.

Ideal Topics For example: computer/operating systems, networks/network forensics, data recovery, analysis, databases, mobile forensics, live data forensics, Windows, Linux and Mac forensics, cryptography, digital forensic tools**, scripting/programming, emerging technologies, law, criminology, court presentation, ethical and professional issues, corporate forensics.

Computing Fundamentals Make sure you understand the fundamentals of computer systems, file systems and networks. These details should be in-depth and should include mathematics such as number systems.

Awareness of Tools Make sure you are aware of the well-known tools used in industry and have some familiarity with using these tools. You should have greater understanding of relevant open source tools to assist application of fundamental theory and knowledge.

Placements If you are able to gain a placement in a relevant role, make sure to take the opportunity. This will give you insight into real-life/practical field experiences and allow you to apply your learning and contextualise the importance of theory and topics on a course.

Placement Alternatives If placements are impossible then industry speakers or companies should be involved in the delivery of your course. Check with your academics to see how many speakers there will be, and the topics.

Context & Application Each module should be applied in the context of digital forensics to facilitate student contextualisation of content and application to real-life scenarios. If you are questioning the relevance of content, ask your lecturers to clarify and provide real-life examples

Be Active If you have guest speakers, competitions, extra lab sessions, etc., make sure to be present and actively involved.

Extra-Curricula Employers look for those with a keen interest in all things computer science, digital forensics and security. They also look favourably on people who have been active beyond their studies. E.g., involvement in the community, having completed extra tasks, learned new skills and those who conduct relevant research outside the scope of the content on their degree.

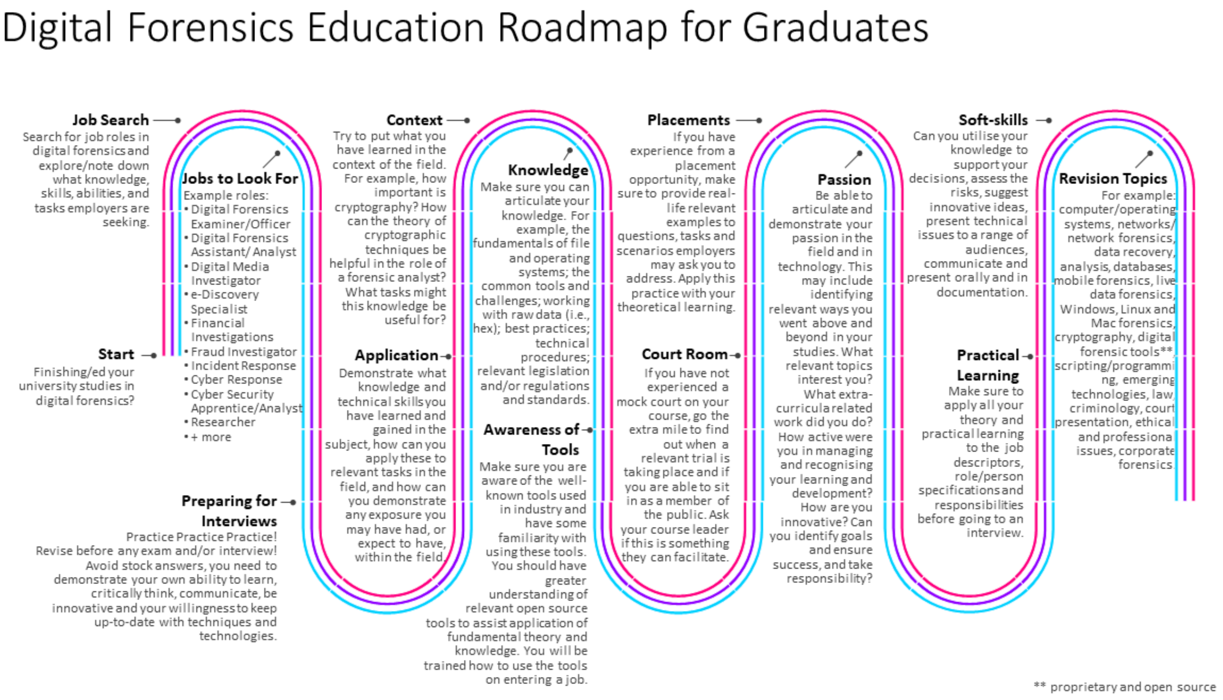
Practical Learning Your course should include a balance between theory & practice. Make sure to complete all hands-on tasks to facilitate your contextualisation and application of the learning materials to real-life.

Learn from Previous Graduates If you get the chance to meet previous graduates ask them to reflect on their learning and tips they can provide you with.

Employability Make sure you receive tailored advice for the field of digital forensics. Make sure you can present yourself clearly, what you have learned, how the course content/subjects apply to real-life, what projects you have completed, how you work in a team and so on. Have a look at recent job advertisements and see what employers are looking for; how do you fit? Practice for interviews and exams with practical components. Make sure you have some examples of your own and that you can demonstrate the basic awareness/fundamentals, in your own words! Do not just regurgitate what your lectures have told you, your peers may do the same! If you cannot identify what you have learned or how it applies on-the-job you will not be successful in an interview.

** proprietary and open source

Figure 10.3 – Digital Forensic Education Roadmap for Students (Final Version)



Digital Forensics Education Roadmap for Graduates

Start Finishing/ed your university studies in digital forensics?

Job Search Search for job roles in digital forensics and explore/note down what knowledge, skills, abilities, and tasks employers are seeking.

Jobs to Look For
Example roles:
- Digital Forensics Examiner/Officer
- Digital Forensics Assistant/ Analyst
- Digital Media Investigator
- e-Discovery Specialist
- Financial Investigations
- Fraud Investigator
- Incident Response
- Cyber Response
- Cyber Security Apprentice/Analyst
- Researcher
- + more

Preparing for Interviews Practice Practice Practice! Revise before any exam and/or interview! Avoid stock answers, you need to demonstrate your own ability to learn, critically think, communicate, be innovative and your willingness to keep up-to-date with techniques and technologies.

Context Try to put what you have learned in the context of the field. For example, how important is cryptography? How can the theory of cryptographic techniques be helpful in the role of a forensic analyst? What tasks might this knowledge be useful for?

Application Demonstrate what knowledge and technical skills you have learned and gained in the subject, how can you apply these to relevant tasks in the field, and how can you demonstrate any exposure you may have had, or expect to have, within the field.

Knowledge Make sure you can articulate your knowledge. For example, the fundamentals of file and operating systems; the common tools and challenges; working with raw data (i.e., hex); best practices; technical procedures; relevant legislation and/or regulations and standards.

Awareness of Tools Make sure you are aware of the well-known tools used in industry and have some familiarity with using these tools. You should have greater understanding of relevant open source tools to assist application of fundamental theory and knowledge. You will be trained how to use the tools on entering a job.

Placements If you have experience from a placement opportunity, make sure to provide real-life relevant examples to questions, tasks and scenarios employers may ask you to address. Apply this practice with your theoretical learning.

Court Room If you have not experienced a mock court on your course, go the extra mile to find out when a relevant trial is taking place and if you are able to sit in as a member of the public. Ask your course leader if this is something they can facilitate.

Passion Be able to articulate and demonstrate your passion in the field and in technology. This may include identifying relevant ways you went above and beyond in your studies. What relevant topics interest you? What extra-curricula related work did you do? How active were you in managing and recognising your learning and development? How are you innovative? Can you identify goals and ensure success, and take responsibility?

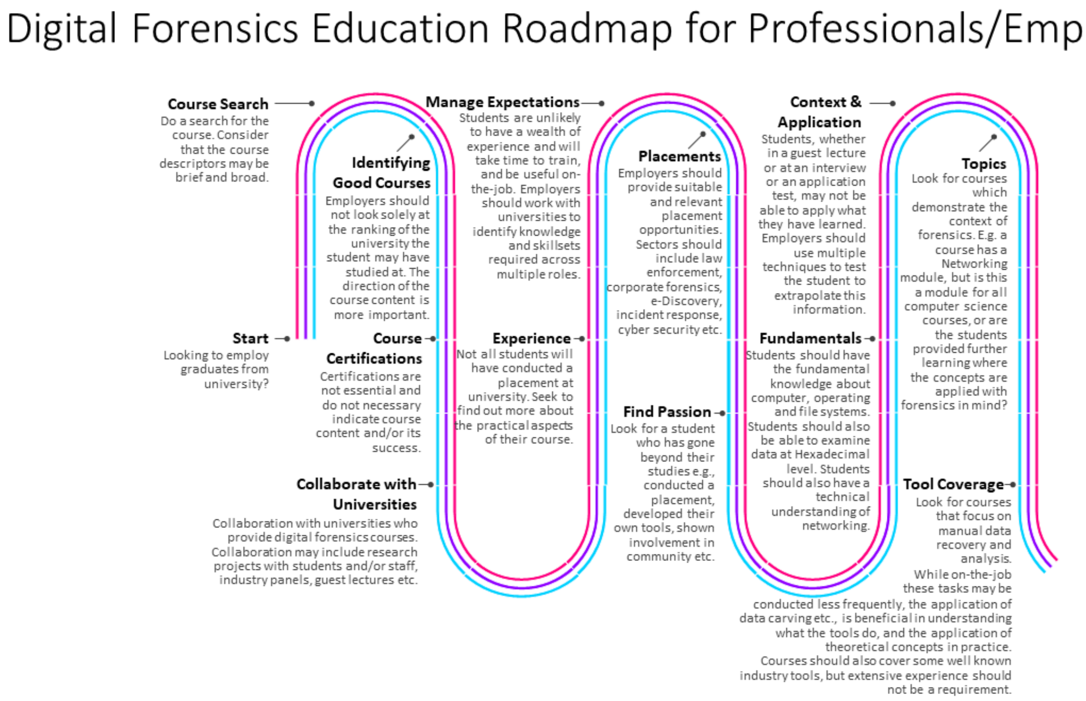
Soft-skills Can you utilise your knowledge to support your decisions, assess the risks, suggest innovative ideas, present technical issues to a range of audiences, communicate and present orally and in documentation.

Practical Learning Make sure to apply all your theory and practical learning to the job descriptors, role/person specifications and responsibilities before going to an interview.

Revision Topics For example: computer/operating systems, networks/network forensics, data recovery, analysis, databases, mobile forensics, live data forensics, Windows, Linux and Mac forensics, cryptography, digital forensic tools**, scripting/programming, emerging technologies, law, criminology, court presentation, ethical and professional issues, corporate forensics.

** proprietary and open source

Figure 10.4 – Digital Forensic Education Roadmap for Graduates (Final Version)



Digital Forensics Education Roadmap for Professionals/Employers

Start
Looking to employ graduates from university?

Course Search
Do a search for the course. Consider that the course descriptors may be brief and broad.

Identifying Good Courses
Employers should not look solely at the ranking of the university the student may have studied at. The direction of the course content is more important.

Course Certifications
Certifications are not essential and do not necessary indicate course content and/or its success.

Collaborate with Universities
Collaboration with universities who provide digital forensics courses. Collaboration may include research projects with students and/or staff, industry panels, guest lectures etc.

Experience
Not all students will have conducted a placement at university. Seek to find out more about the practical aspects of their course.

Manage Expectations
Students are unlikely to have a wealth of experience and will take time to train, and be useful on-the-job. Employers should work with universities to identify knowledge and skillsets required across multiple roles.

Placements
Employers should provide suitable and relevant placement opportunities. Sectors should include law enforcement, corporate forensics, e-Discovery, incident response, cyber security etc.

Find Passion
Look for a student who has gone beyond their studies e.g., conducted a placement, developed their own tools, shown involvement in community etc.

Fundamentals
Students should have the fundamental knowledge about computer, operating and file systems. Students should also be able to examine data at Hexadecimal level. Students should also have a technical understanding of networking.

Context & Application
Students, whether in a guest lecture or at an interview or an application test, may not be able to apply what they have learned. Employers should use multiple techniques to test the student to extrapolate this information.

Topics
Look for courses which demonstrate the context of forensics. E.g. a course has a Networking module, but is this a module for all computer science courses, or are the students provided further learning where the concepts are applied with forensics in mind?

Tool Coverage
Look for courses that focus on manual data recovery and analysis. While on-the-job these tasks may be conducted less frequently, the application of data carving etc., is beneficial in understanding what the tools do, and the application of theoretical concepts in practice. Courses should also cover some well known industry tools, but extensive experience should not be a requirement.

Figure 10.5 – Digital Forensic Education Roadmap for Professionals/Employers (Final Version)

10.4 Further Research

This section converses future work ideas for the wider community based on thesis results and the continuous advancements and challenges which face digital forensics.

As a focus works should continue to examine the suitability and sustainability of degree programmes in digital forensics considering most recent shifts towards cyber security. In particular, the analysis and examination of the impact and worth of newly devised educational and certification frameworks in cyber security and, by extension, digital forensics should be considered. For example, research into how certification standards such as the NCSC Certifications in the UK for cyber security and digital forensic programmes were devised, what stakeholder views and experiences they consider, how sustainable they are and the effect they have on educational programmes versus their worth to employers, students and academics. An issue with current educational programmes is often the lack of clarity on course contents for both applicants and employers, as documented in this thesis. Consequently, do newly devised certifications and standards assist in adding value and clarity to course coverage; question may for example, include:

– what is the uptake by courses?
– have the certified courses improved?

- have the skills and knowledge of graduates improved and have certifications affected employability of graduates?
- are the graduates more effective and able to apply their learning more comprehensively addressing issues of contextualisation and awareness?
- how can the frameworks be improved and are they sustainable in a continually developing and highly technical discipline?
- do the frameworks address the views of multiple stakeholders with interests in digital forensics, beyond those involved in the delivery of such works?

Furthermore, the literature would benefit from an in-depth analysis of content of higher education programmes and training offerings at material level, beyond the examination by module naming convention and course descriptors, as conducted in this thesis. These should include collaboration within academia, industry, proprietary training and continuing professional development settings to identify specialisms which are currently ill-addressed within learning. Analysis of programme content for mobile forensics, network forensics, live data forensics, cloud forensics and malware analysis should be considered top priorities. Analysis should consider course content, aims and goals, objectives, expectations and outcomes and achievements. This examination should include teaching and training observations, where assessment of the applicability of theory and practice of students and professionals in their learning setting should be considered. The researcher of this study believes, this will go some way to identifying the state of the discipline at a much deeper level to address several skills-shortages and provide institutions with developments reflective of ever-changing real-life demands and expectations. The researcher appreciates this task may be unmanageable and unattainable across the discipline and therefore educators and trainers should incorporate the contribution of more stakeholders (professionals and alumni) in the curriculum development/revision process and delivery of courses.

As the demands for skilled practitioners in areas such as mobile, live and Mac forensics and malware analysis using advanced digital forensic techniques grows education and training programmes should be assessed and revised with stakeholder needs analysis in mind. Two professional views which stand out within this research cover one central issue of education, training, and digital forensic graduates:

- "It can take 1-2 years for a graduate to be effective, which also represents a resource drain on existing staff. More field experience would be very beneficial, but extremely hard to come by. Some form of apprenticeship/work experience would be beneficial."
- "Much of what is covered is theory based and students come from university with very little idea as to how to actually do specific tasks."

Future works should consider how the delivery and hands-on experience of forensics in practice could improve within digital forensics education and training. This may include improved placement opportunities, apprenticeship schemes, university courses with on-the-job learning and training akin to medical education and, innovative learning methods. Moreover, these works should consider the CDIO (Conceive, Design, Implement, Operate) education model applied to digital forensics education, something which is relatively unexplored within the literature of this discipline. Work should explore curriculum materials as well as students and educators within various learning situations and the effect and improvement this model may provide for skills-shortages in the practice of digital forensics.

In addition, the author of this study believes further research on the development of a tool used to create datasets and scenarios is viable. An educational tool which looks to help educators and trainers alike to create and store scenarios and case studies in a multitude of crimes for the purposes of education and training within digital forensics. The future development which should be extended to include a range of features among those from existing works and be used to create a more comprehensive and collaborative toolset. The tool should not only consider the development of a range of images and fabricated data but, as well, appropriate documentation and questions relating to each scenario. This work should be a collaborative effort and include practitioners who may be able to provide real-life scenarios and shed light on difficulties faced by forensics practitioners to give students close to relevant working examples and practice. This idea should be considered by current digital forensic working groups, authorities and training bodies involved within the discipline to identify its feasibility and access issues.

A key contribution of this research includes the digital forensic education roadmaps discussed in chapter 9. Works that could enhance the roadmaps, and should be considered further work, include the reduction of text so that the diagram still provide clarity and meaning. The addition of a cyclical approach to the roadmap for educators to consider the sustainability of a course or the re-design and development of an existing programme. The researcher also identifies that the student roadmap may benefit from consideration of different types of students, study levels, student backgrounds, and extend to the delivery of education/training for industry professionals. In addition, the relevance of the public as a stakeholder in education should be considered further. Further works should at how education establishments, training providers, and so on should publish detailed roadmaps that outline the processes, collaborations, content, placements or alternatives and employability factors in a standardised form that is readily available for students/employers as reference each year.

10.5 Summary

Digital forensics is now a field of knowledge for everyone working on investigations where digital devices are present, be it criminal or corporate environments. The target audience for digital forensics is broad due to its interdisciplinary approach, therefore this thesis considered and has drawn together five important stakeholder groups within digital forensics education: academics, graduates, students, professionals, and the public. This research has highlighted expectations of an individual with a degree in digital forensics such as, basic technical knowledge and skills of computers and forensics, programming and scripting skills, understanding and technical abilities to work with a range of file systems and operating systems including Windows, Linux and Mac, greater knowhow to conduct mobile forensics, and increasingly the need to address issues centered on the lack of experience and difficulties with awareness and contextualisation of learning and applicability to the discipline and practice on behalf of graduates, students and academics. Themes ascertained from this research predominately include the need for experience, the position of digital forensics in academia and wider, as well as the difficulties in awareness. These have become the main focus of this work, principally the development of topics and skills mentioned throughout this thesis revolve around the ability to develop longstanding investigative and analysis skills in order to demonstrate an analytical mind-set, initiative, problem-solving, decision-making, communicative skills, critical and creative thinking skills, and the professional and further soft skills expected in a workplace to produce a well-rounded digital forensic professional. Finally, as a rich and distinct discipline faces continual challenges within industry and the education sector, this thesis argues that digital forensics programmes should be designed to reflect and consider a wider range of stakeholder opinions to produce the most effective individuals for employability within the field of digital forensics and provides suggestions as a model for how curriculum designers may work towards this.

REFERENCES

AccessData (2015) *Forensic Toolkit (FTK)*. AccessData. Available at: http://accessdata.com/ (Accessed: 17 December 2015).

ACPO (2012) *ACPO Good Practice Guide for Digital Evidence*. London: Association of Chief Police Officers. Available at: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (Accessed: 1 January 2015).

Adams, A. and Cox, A. L. (2008) 'Questionnaires, in-depth interviews and focus groups', in Cairns, P. and Cox, A. L. (eds) *Research Methods for Human–Computer Interaction*. Cambridge: Cambridge University Press, pp. 17–34. doi: 10.1017/CBO9780511814570.003.

Adams, W. C. (2015) 'Conducting Semi-Structured Interviews', in Newcomer, K. E., Hatry, H. P., and Wholey, J. S. (eds) *Handbook of Practical Program Evaluation*. 4th edn. Hoboken, NJ, USA: John Wiley & Sons, Inc., pp. 492–505. doi: 10.1002/9781119171386.ch19.

Adelstein, F., Gao, Y. and Richard III, G. G. (2005) 'Automatically Creating Realistic Targets for Digital Forensics Investigation', in *Digital Forensic Research Workshop (DFRWS)*. New Orelans, LA: Digital Forensic Research Workshop (DFRWS). Available at: https://www.dfrws.org/2005/proceedings/adelstein_falcon.pdf (Accessed: 11 January 2016).

Ahmad, A. and Maynard, S. (2014) 'Teaching information security management: reflections and experiences', *Information Management & Computer Security*, 22(5), pp. 513–536. doi: 10.1108/IMCS-08-2013-0058.

Aldawood, H. and Skinner, G. (2018) 'Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review', in *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*. *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, pp. 62–68. doi: 10.1109/TALE.2018.8615162.

Alharbi, S., Weber-Jahnke, J. and Traore, I. (2011) 'The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review', in Kim, T. et al. (eds) *Information Security and Assurance*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 87–100. doi: 10.1007/978-3-642-23141-4_9.

Alqahtany, S. *et al.* (2016) 'A forensic acquisition and analysis system for IaaS', *Cluster Computing*, 19(1), pp. 439–453. doi: 10.1007/s10586-015-0509-x.

Alva, A. and Endicott-Popovsky, B. (2012) 'Digital Evidence Education in Schools of Law', *Journal of Digital Forensics, Security and Law*, 7(2), pp. 75–88.

Anderson, P. *et al.* (2006) 'A Comparative Study of Teaching Forensics at a University Degree Level.', in *IMF. IT-Incidents Management & IT-Forensics*, Stuttgart, pp. 116–127.

Andrews, J. and Higson, H. (2008) 'Graduate Employability, "Soft Skills" Versus "Hard" Business Knowledge: A European Study', *Higher Education in Europe*, 33(4), pp. 411–422. doi: 10.1080/03797720802522627.

Angelopoulou, O. and Vidalis, S. (2015) ‘An academic approach to digital forensics’, *Journal of Information Warfare*, 13(4). Available at: http://researchprofiles.herts.ac.uk/portal/files/10607202/JIW_Angelopoulou_Vidalis.docx (Accessed: 7 May 2017).

Atieno, O. P. (2009) ‘An Analysis of the Strengths and Limitation of Qualitative and Quantitative Research Paradigms’, *Problems of Education in the 21st century*, 13, p. 6.

Aytes, K. and Connolly, T. (2004) ‘Computer Security and Risky Computing Practices: A Rational Choice Perspective’, *Journal of Organizational and End User Computing*, 16(3), pp. 22–40.

Aytes, K. and Conolly, T. (2003) ‘A Research Model for Investigating Human Behavior Related to Computer Security’, in *Proceedings of the 9th Americas Conference on Information Systems*. Tampa, FL: Association for Information Systems (AIS). Available at: https://aisel.aisnet.org/amcis2003/260 (Accessed: 22 February 2019).

Bagby, J. and Ruhnka, J. (2006) ‘Development and Delivery of Coursework: The Legal\slash Regulatory\slash Policy Environment of Cyberforensics’, *Journal of Digital Forensics, Security and Law*, 1(2), pp. 39–74.

Baguelin, F. *et al.* (2013) *Digital Forensics Framework*. ArxSys. Available at: http://www.arxsys.fr/discover/ (Accessed: 5 January 2016).

Barnes, C. (2014) ‘Education and Training - What’s the difference?’, *eLearning Industry*, 13 June. Available at: https://elearningindustry.com/education-and-training-what-is-the-difference (Accessed: 17 February 2019).

Barrows, H. S. (1988) ‘The Tutorial Process’, in. Springfield, IL: Southern Illinois University School of Medicine. Available at: https://onlinelibrary.wiley.com/doi/abs/10.1016/0307-4412%2889%2990116-7 (Accessed: 17 February 2019).

Beardmore, P., Fellows, G. and Sommer, P. (2017) ‘UK ISO 17025 Digital Forensics Survey April 2017: Results’. Available at: http://digital-evidence.expert/UK%20ISO%2017025%20Digital%20Forensics%20Survey%20April%202017.pdf (Accessed: 5 November 2018).

Beckett, J. and Slay, J. (2011) ‘Scientific underpinnings and background to standards and accreditation in digital forensics’, *Digital Investigation*, 8(2), pp. 114–121. doi: 10.1016/j.diin.2011.08.001.

Beebe, N. (2009) ‘Digital Forensic Research: The Good, the Bad and the Unaddressed’, in Peterson, G. and Shenoi, S. (eds) *Advances in Digital Forensics V*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 17–36. doi: 10.1007/978-3-642-04155-6_2.

Bennett, R. *et al.* (2008) ‘Reassessing the value of work-experience placements in the context of widening participation in higher education’, *Journal of Vocational Education & Training*, 60(2), pp. 105–122. doi: 10.1080/13636820802042339.

Big Brother Watch (2017) *Police Access to Digital Evidence*. London: Big Brother Watch. Available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2017/11/Police-Access-to-Digital-Evidence-1.pdf (Accessed: 19 January 2018).

Biggs, J. (1999) ‘What the Student Does: teaching for enhanced learning’, *Higher Education Research & Development*, 18(1), pp. 57–75. doi: 10.1080/0729436990180105.

Bond Solon (2019) *Bond Solon - The legal training company*, *Bond Solon*. Available at: https://www.bondsolon.com/ (Accessed: 21 February 2019).

Boyatzis, R. E. (1998) *Transforming Qualitative Information: Thematic Analysis and Code Development*. Thousand Oaks, CA: SAGE.

Brace, I. (2008) *Questionnaire Design: How to Plan, Structure and Write Survey Material for Effective Market Research*. Kogan Page Publishers.

Brennecke, A. and Schumann, H. (2009) *A general framework for digital game-based training systems*. University of Rostock. Available at: http://www.informatik.uni-rostock.de/schumann/papers/2008+/Angela_GET.pdf (Accessed: 7 January 2016).

Buchler, N. *et al.* (2018) ‘Sociometrics and observational assessment of teaming and leadership in a cyber security defense competition’, *Computers & Security*, 73, pp. 114–136. doi: 10.1016/j.cose.2017.10.013.

Cabinet Office (2016) *National Cyber Security Strategy 2016-2021*. London: HM Government, p. 80. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (Accessed: 8 August 2018).

Cambridge University Press (2013) ‘keyboard warrior, n.’, *Cambridge Advanced Learner’s Dictionary and Thesaurus*. 4th edn. Cambridge: Cambridge University Press. Available at: https://dictionary.cambridge.org/dictionary/english/keyboard-warrior (Accessed: 22 February 2019).

Carmichael, S. (2019) *Why you should consider a two-year degree*, *UCAS*. Available at: https://www.ucas.com/connect/blogs/why-you-should-consider-two-year-degree (Accessed: 19 March 2019).

Carrier, B. (2015) *The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools*. Available at: http://www.sleuthkit.org/ (Accessed: 21 December 2015).

Carter, J. and Coupland, S. (2014) ‘Robotics for Distance learning: A Case Study from a UK Masters Programme’. Available at: https://www.dora.dmu.ac.uk/handle/2086/10844 (Accessed: 15 April 2015).

Cellan-Jones, R. (2014) ‘Prison data loss leads to large fine’, *BBC News*. Online, 26 August. Available at: https://www.bbc.com/news/technology-28936396 (Accessed: 4 March 2018).

Champagne, A. (2015) ‘Digital Forensics Policy: Expectations and Acceptance’, *Evidence Technology Magazine*, April, pp. 16–18.

Chawki, M. *et al.* (2015) *Cybercrime, Digital Forensics and Jurisdiction*. Springer.

Chen, T., Hu, W. and Shi, Q. (2009) ‘Teaching reform of information security curriculum of distance learning’, in *Education Technology and Computer Science, 2009. ETCS’09. First International Workshop on*. IEEE, pp. 185–189. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4958752 (Accessed: 8 April 2015).

Chui, W. H. (2009) ‘First practice placement: Great expectation and anxiety of a cohort of social work students’, *The Journal of Practice Teaching and Learning*, 9(2), pp. 10–32. doi: 10.1921/146066910X518085.

Cigoj, P. and Blažič, B. J. (2016) ‘An Advanced Educational Tool for Digital Forensic Engineering’, *International Journal of Emerging Technologies in Learning (iJET)*, 11(03), pp. 15–23. doi: 10.3991/ijet.v11i03.5294.

Clarke, V. and Braun, V. (2013) ‘Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning.’, *The Psychologist*, 26(2), pp. 120–123.

Clough, J. (2014) ‘A world of difference: The Budapest convention on Cybercrime and the challenges of Harmonisation’, *Monash University Law Review*, 40(3), p. 698.

Codecademy (2018) *Codecademy*, *Codecademy*. Available at: https://www.codecademy.com/catalog/subject/all (Accessed: 18 December 2018).

Coe, R. *et al.* (2017) *Research Methods and Methodologies in Education*. 2nd edn. Thousand Oaks, CA: SAGE.

College of Policing (2016) ‘Competency and Values Framework for Policing’. College of Policing. Available at: https://d17wy4t6ps30xx.cloudfront.net/production/uploads/2017/09/Competency-and-Values-Framework-for-Policing_4.11.16.pdf (Accessed: 28 August 2018).

College of Policing (2018a) *Professional Profiles*, *College of Policing*. Available at: https://profdev.college.police.uk/professional-profiles/ (Accessed: 28 August 2018).

College of Policing (2018b) ‘Trial Draft Policing Professional Profile - Digital Media Investigation Co-ordinator’. College of Policing. Available at: https://d17wy4t6ps30xx.cloudfront.net/production/uploads/2018/04/INT-COMD-TL-Digital-Media-Investigation-Co-ordinator-V1.0-Trial-Draft-April-18.pdf (Accessed: 28 August 2018).

College of Policing (2018c) ‘Trial Draft Policing Professional Profile - Digital Media Investigator’. College of Policing. Available at: https://d17wy4t6ps30xx.cloudfront.net/production/uploads/2018/04/INT-COMD-SD-Digital-Media-Investigator-V1.0-Trial-Draft-April-18.pdf (Accessed: 28 August 2018).

College of Policing (2018d) ‘Uploaded Policing Professional Profiles - Including both Final Versions and Trial Drafts’. College of Policing. Available at: https://d17wy4t6ps30xx.cloudfront.net/production/uploads/2018/11/PPP-Trial-drafts-and-final-version-upload-list-v2.0-November-2018-1.pdf (Accessed: 18 December 2018).

Communications-Electronics Security Group and Centre for the Protection of National Infrastructure (2015) *Password Guidance: Simplifying your approach*. London: National Cyber Security Centre (NCSC), GCHQ. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf (Accessed: 22 February 2019).

Conti, M. *et al.* (2018) ‘Internet of Things security and forensics: Challenges and opportunities’, *Future Generation Computer Systems*, 78, pp. 544–546. doi: 10.1016/j.future.2017.07.060.

Council of Europe (2001) ‘Convention on Cybercrime’, (No. 185). Available at: http://window.dev.informika.ru/resource/378/65378/files/m08-10.pdf (Accessed: 4 January 2016).

Council of Europe (2014) *Law Enforcement Training Strategy Project area specific strategies*. The Hague, The Netherlands: Europol. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168030287b (Accessed: 4 January 2016).

Council of Europe (2016) *General Data Protection Regulation (GDPR) 95/46/EC*, *Council Regulation (EC)*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Accessed: 10 June 2017).

Council Regulation (EU) 2016/679 (2016) 'Council regulation (EU) 2016/679 on the protection of natural persons with regard to processing of personal data and on free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)', *Official Journal*, L119/1. Available at: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

Craig, D. V. (2009) *Action Research Essentials*. John Wiley & Sons.

Crellin, J., Adda, M. and Duke-Williams, E. (2010) 'The use of simulation in digital forensics teaching', in *11th Annual Conference of the Higher Education Academy, Information and Computer Science Group*. Durham, UK.

Creswell, J. W. (2014) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 4th edn. SAGE.

Creswell, J. W. and Creswell, J. D. (2017) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.

Creswell, J. W. and Poth, C. N. (2016) *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. 4th edn. Thousand Oaks, CA: SAGE Publications. Available at: https://books.google.co.uk/books?id=bOLFDQAAQBAJ&printsec=frontcover.

Dafoulas, G. A., Neilson, D. and Hara, S. (2017) 'State of the Art in Computer Forensic Education-A Review of Computer Forensic Programmes in the UK, Europe and US', in. IEEE, pp. 144–154. doi: 10.1109/ICTCS.2017.65.

Data Protection Act 1998 (2005) *Data Protection Act 1998: Elizabeth II. 1998. Chapter 29*. London: Stationery Office. Available at: https://www.legislation.gov.uk/ukpga/1998/29/contents (Accessed: 4 March 2018).

Data Protection Act 2018 (2018). Available at: http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf (Accessed: 21 February 2019).

Denham, E. (2017) 'GDPR – sorting the fact from the fiction', *ICO Blog*, 9 August. Available at: https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/ (Accessed: 4 March 2018).

Denscombe, M. (2014) *The Good Research Guide: For Small-Scale Social Research Projects*. 5th edn. Berkshire, England: McGraw-Hill Education (UK).

Department for Culture, Media & Sport (2018) *Cyber Security Breaches Survey 2018 Report*. Statistical Release. London, United Kingdom: Ipos MORI and The Institute for Criminal Justice Studies at the University of Portsmouth. Available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf.

Dezfoli, F. N. *et al.* (2013) 'Digital Forensic Trends and Future', *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 2(2), pp. 48–76.

DFRWS (2001) 'A Road Map for Digital Forensic Research', in *Report From the First Digital Forensic Research Workshop (DFRWS)*. *The Digital Forensic Research Conference*, Utica, NY, USA: DFRWS. Available at: http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf (Accessed: 10 May 2017).

Digital Continuity to Support Forensic Readiness (2011) *Digital Continuity to Support Forensic Readiness*. 1.2. Surrey, United Kingdom: The National Archives. Available at: https://www.nationalarchives.gov.uk/documents/information-management/forensic-readiness.pdf (Accessed: 25 June 2020).

Digital Corpora (2017) *Digital Corpora*, *DigitalCorpora.org*. Available at: http://digitalcorpora.org/ (Accessed: 10 May 2017).

Disney, R. and Simpson, P. (2017) *Police workforce and funding in England and Wales*. Edited by J. Payne. United Kingdom: The Institute for Fiscal Studies (BN208). Available at: https://www.ifs.org.uk/uploads/publications/bns/bn208.pdf (Accessed: 13 February 2018).

Dlamini, M. T., Eloff, J. H. P. and Eloff, M. M. (2009) 'Information security: The moving target', *Computers & Security*, 28(3–4), pp. 189–198. doi: 10.1016/j.cose.2008.11.007.

Dlamini, M., Venter, H. and Eloff, M. (2014) 'Requirements for Preparing the Cloud to Become Ready for Digital Forensic Investigation', in *Proceedings of the 13th European Conference on Cyber Warfare and Security*. *European Conference on Cyber Warfare and Security*, The University of Piraeus, Greece: Academic Conferences and Publishing International Limited, pp. 242–250. Available at: https://cryptome.org/2014/12/ECCWS2014.pdf (Accessed: 30 August 2018).

Douglas, J., Douglas, A. and Barnes, B. (2006) 'Measuring student satisfaction at a UK university', *Quality Assurance in Education*, 14(3), pp. 251–267. doi: 10.1108/09684880610678568.

Drange, T., Irons, A. and Drange, K. (2017) 'Creativity in the Digital Forensics Curriculum':, in *Proceedings of the 9th International Conference on Computer Supported Education*. *9th International Conference on Computer Supported Education*, Porto, Portugal: SCITEPRESS - Science and Technology Publications, pp. 103–108. doi: 10.5220/0006294101030108.

Du, X., Le-Khac, N.-A. and Scanlon, M. (2017) 'Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service', in *European Conference on Cyber Warfare and Security*. *ECCWS*, Dublin, Ireland, p. 10. Available at: https://arxiv.org/ftp/arxiv/papers/1708/1708.01730.pdf (Accessed: 15 October 2017).

Duncan, K. (2018) *The Diagrams Book: 60 ways to solve any problem visually*. 2nd edn. LID Editorial.

Dunn Cavelty, M. (2014) 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities', *Science and Engineering Ethics*, 20(3), pp. 701–715. doi: 10.1007/s11948-014-9551-y.

Edinburgh Napier University (2018) *National Cyber Security Centre certifies course: GCHQ backing for BEng (Hons) in Cybersecurity and Forensics*, *Edinburgh Napier University*. Available at: https://www.napier.ac.uk:443/about-us/news/ncsccertification/ (Accessed: 15 February 2019).

Efron, S. E. and Ravid, R. (2013) *Action Research in Education: A Practical Guide*. New York, NY: Guilford Press.

European Commission (2013) *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Available at: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (Accessed: 8 August 2018).

European Commission (2016) *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (Accessed: 8 August 2018).

European Commission (2018) 'Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine', *European Commission Press Release Database*, 18 July. Available at: http://europa.eu/rapid/press-release_IP-18-4581_en.htm (Accessed: 15 August 2018).

European Cybercrime Training and Education Group (2019) *ECTEG Courses*. Available at: https://www.ecteg.eu/course-packages/ (Accessed: 4 January 2019).

European Parliament (2017) *European Parliament resolution of 3 October 2017 on the fight against cybercrime*. Strasbourg: European Parliament. Available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2017-0366&format=XML&language=EN (Accessed: 25 February 2019).

Fahdi, M. A., Clarke, N. L. and Furnell, S. M. (2013) 'Challenges to digital forensics: A survey of researchers amp; practitioners attitudes and opinions', in *2013 Information Security for South Africa*. *2013 Information Security for South Africa*, pp. 1–8. doi: 10.1109/ISSA.2013.6641058.

Field, A. (2005) 'C8057 (Research Methods II): Factor Analysis on SPSS'. University of Sussex. Available at: http://users.sussex.ac.uk/~andyf/factor.pdf (Accessed: 11 June 2017).

Field, A. (2013) *Discovering Statistics Using IBM SPSS Statistics*. 4th edn. SAGE.

Flick, U. (2008) *Managing Quality in Qualitative Research*. SAGE.

Flick, U. (2014) *An Introduction to Qualitative Research*. 5th edn. SAGE.

Flick, U. (2017) *The SAGE Handbook of Qualitative Data Collection*. SAGE.

Floyd, K. and Yerby, J. (2014) 'Development of a Digital Forensics Lab to Support Active Learning', in *SAIS 2014 Proceedings*. Association for Information Systems (AIS), p. 7. Available at: https://aisel.aisnet.org/cgi/viewcontent.cgi?referer=https://scholar.google.co.uk/&httpsredir=1&article=1006&amp;context=sais2014 (Accessed: 9 February 2019).

Foddy, W. and Foddy, W. H. (1994) *Constructing Questions for Interviews and Questionnaires: Theory and Practice in Social Research*. Cambridge University Press.

Forensic Focus (no date) 'Test Images and Forensic Challenges', *Forensic Focus*. Available at: http://www.forensicfocus.com/images-and-challenges (Accessed: 10 December 2018).

Forensic Focus (2013) 'Forensic Student - In need of sponsor/client - Digital Forensics Forums', *Forensic Focus*. Available at: https://www.forensicfocus.com/Forums/viewtopic/t=11023/postdays=0/postorder=asc/start=0/ (Accessed: 10 December 2018).

Franke, K. and Srihari, S. (2008) 'Computational Forensics: Towards Hybrid-Intelligent Crime Investigation', in *Proceedings of IWCF: International Workshop on Computational Forensics*. Manchester, UK: Springer, pp. 300–324. doi: 10.1016/j.artint.2007.06.005.

Frost & Sullivan (2017) *The 2017 Global Information Security Workforce Study: Women in Cybersecurity*. White Paper. Santa Clara, CA: Frost & Sullivan. Available at: https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf (Accessed: 15 October 2018).

Furnell, S. and Kaspersky, E. (2014) 'A security education Q&A', *Information Management & Computer Security*, 22(2), pp. 130–133. doi: 10.1108/IMCS-01-2014-0006.

Garfinkel, S. *et al.* (2009) 'Bringing science to digital forensics with standardized forensic corpora', *Digital Investigation*, 6, pp. S2–S11. doi: 10.1016/j.diin.2009.06.016.

Garfinkel, S. (2010) 'Digital forensics research: The next 10 years', *Digital Investigation*, 7, pp. S64–S73. doi: 10.1016/j.diin.2010.05.009.

Garrison, D. R. (1997) 'Self-Directed Learning: Toward a Comprehensive Model', *Adult Education Quarterly*, 48(1), pp. 18–33. doi: 10.1177/074171369704800103.

GCHQ (2016) *GCHQ certifies six more Masters' degrees in Cyber Security*. Available at: https://www.gchq.gov.uk/news-article/gchq-certifies-six-more-masters-degrees-cyber-security (Accessed: 17 August 2018).

Gemalto (2018) *2017: The Year of Internal Threats and Acidental Data Breaches Findings from the 2017 Breach Level Index*. Gemalto. Available at: https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf (Accessed: 15 August 2018).

Genoe, R., Toolan, F. and McGourty, J. (2014) 'Programming for Investigators: From Zero to Hero in 4 Days', in. *Cybercrime Forensics, Education and Training (CFET)*, Canterbury Christ Church University. Available at: https://www.researchgate.net/publication/271511408_Programming_for_Investigators_From_Zero_to_Hero_in_Four_Days.

Gillham, B. (2008) *Developing a Questionnaire*. A&C Black. Available at: https://books.google.co.uk/books?id=EpKvAwAAQBAJ&printsec=frontcover (Accessed: 30 August 2018).

Ginty, C. and Boland, J. (2016) 'Supporting the first year experience in Higher Education in Ireland: Impact on Student Engagement, Teaching Practice and Institutional Policy.', *Student Engagement and Experience Journal*, 5(1), p. 47. doi: 10.7190/seej.v4i1.119.

Glaser, B. G. and Strauss, A. L. (2009) *The discovery of grounded theory: strategies for qualitative research*. New Brunswick: Aldine.

Gomez, L. S. M. (2012) 'Triage in-Lab: case backlog reduction with forensic digital profiling', in *Proceedings of the Argentine Conference on Informatics and Argentine Symposium on Computing and Law*, pp. 217–225. Available at: http://41jaiio.sadio.org.ar/sites/default/files/17_SID_2012.pdf (Accessed: 21 December 2015).

Google (2019a) *Explore search interest for Artificial Intelligence (Field of Study and Search Term) Worldwide from 2004*, *Google Trends*. Available at: https://trends.google.com/trends/explore?date=2004-01-01%202019-01-02&q=%2Fm%2F0mkz,artificial%20intelligence (Accessed: 2 January 2019).

Google (2019b) *Explore search interest for Internet of Things (Field of Study and Search Term) Worldwide from 2004*, *Google Trends*. Available at: https://trends.google.com/trends/explore?date=all&q=%2Fm%2F02vnd10,Internet%20of%20things/trends/explore (Accessed: 2 January 2019).

Google Scholar Metrics (no datea) *Digital Investigation - Google Scholar Metrics Search*. Available at: https://scholar.google.co.uk/citations?hl=en&view_op=search_venues&vq=digital+investigation&btnG= (Accessed: 13 February 2019).

Google Scholar Metrics (no dateb) *Forensic Science Journal Rankings*. Available at: https://scholar.google.co.uk/citations?view_op=top_venues&hl=en&vq=soc_forensicscience (Accessed: 13 February 2019).

Govan, M. (2016) 'The application of peer teaching in digital forensics education', *Higher Education Pedagogies*, 1(1), pp. 57–63. doi: 10.1080/23752696.2015.1134198.

Greathead, D. (2008) 'MBTI Personality Type and Student Code Comprehension Skill', in *Proc. 20th Work. Psychol. Psychology of Programming Interest Group (PPIG)*, Lancaster, UK: PPIG. Available at: http://www.ppig.org/sites/default/files/2008-PPIG-20th-greathead.pdf (Accessed: 25 January 2019).

Gregal, H. (2014) 'Cyber Security and Digital Forensics: Two Sides of the Same Coin', *The Leahy Center for Digital Investigation (LCDI)*, 22 October. Available at: https://lcdiblog.champlain.edu/2014/10/22/cyber-security-digital-forensics-two-sides-coin/ (Accessed: 9 February 2019).

Grobler, C. and Louwrens, B. (2006) 'Digital forensics: a multi-dimensional discipline', in *Proceedings of the ISSA 2006*. *Insight to Foresight Conference*, Pretoria: University of Pretoria.

Grobler, M. (2010) 'Digital Forensic Standards: International Progress', in *Proceedings of the South African Information Security Multi-Conference*. *SAISMC*, Port Elizabeth, South Africa: Centre for Security, Communications & Network Research, University of Plymouth, pp. 261–271. Available at: http://researchspace.csir.co.za/dspace/bitstream/handle/10204/4108/GROBLER%20_2010.pdf?sequence=1 (Accessed: 20 June 2016).

Grobler, M. (2012) 'The Need for Digital Evidence Standardisation', *International Journal of Digital Crime and Forensics*, 4(2), pp. 1–12. doi: 10.4018/jdcf.201204010110.1016/S0960-9822(97)70976-X.

Grobler, M. and Dlamini, I. (2010) 'Managing digital evidence-the governance of digital forensic', *Journal of Contemporary Management*, 7(1), pp. 1–21.

Groves, R. M. *et al.* (2009) *Survey Methodology*. 2nd edn. Hoboken, New Jersey: John Wiley & Sons. Available at: https://books.google.co.uk/books?id=HXoSpXvo3s4C&printsec=frontcover.

Grow, G. O. (1991) ‘Teaching Learners To Be Self-Directed’, *Adult Education Quarterly*, 41(3), pp. 125–149.

Guidance Software (2015) *EnCase Forensic*. Guidance Software. Available at: https://www2.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx (Accessed: 17 December 2015).

Halpern, D. F. and Hakel, M. D. (2003) ‘Applying the Science of Learning to the University and Beyond: Teaching for Long-Term Retention and Transfer’, *Change: The Magazine of Higher Learning*, 35(4), pp. 36–41. doi: 10.1080/00091380309604109.

Hamari, J., Koivisto, J. and Sarsa, H. (2014) ‘Does Gamification Work? – A Literature Review of Empirical Studies on Gamification’, in. *47th Hawaii International Conference on System Science*, IEEE, pp. 3025–3034. doi: 10.1109/HICSS.2014.377.

Hargreaves, C. and Prince, D. (2013) ‘Understanding cyber criminals and measuring their future activity’. Available at: http://eprints.lancs.ac.uk/65477/1/Final_version_Understanding_cyber_criminals_and_measuring_their_activity.pdf (Accessed: 29 December 2015).

Hargreaves, J., Husband, H. and Linehan, C. (2018) *Police Workforce, England and Wales, 31 March 2018*. London, United Kingdom: Home Office and Office for National Statistics (Statistical Bulletin 11/18). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/726401/hosb1118-police-workforce.pdf (Accessed: 15 October 2018).

Harichandran, V. S. *et al.* (2016) ‘A cyber forensics needs analysis survey: Revisiting the domain’s needs a decade later’, *Computers & Security*, 57, pp. 1–13. doi: 10.1016/j.cose.2015.10.007.

Harreveld, B. and Singh, M. (2009) ‘Contextualising learning at the education-training-work interface’, *Education + Training*, 51(2), pp. 92–107. doi: 10.1108/00400910910941264.

Hegarty, R., Lamb, D. and Attwood, A. (2014) ‘Digital Evidence Challenges in the Internet of Things’, in *Proceedings of the Tenth International Network Conference (INC 2014)*. Lulu. com, p. 163. Available at: https://books.google.com/books?hl=en&lr=&id=Tl7qBgAAQBAJ&oi=fnd&pg=PA163&dq=%22state%3B+idle+or%22+%22overview+of+the+general+digital+forensics+literature+to+illustrate+where%22+%22enforcement+agencies,+private+organisations+and+even+individuals+are%22+%22for+investigations+in+the+IoT+by+first+considering+the+seminal+work%22+&ots=LySLpySx3l&sig=jvwUR3KTrQVzoE-v-nCtQwrl6OE (Accessed: 3 July 2015).

Hénard, F. and Roseveare, D. (2012) *Fostering Quality Teaching in Higher Education: Policies and Practices: An Institutional Management in Higher Education (IMHE) Guide for Higher Education Institutions*. The Organisation for Economic Co-operation and Development (OECD). Available at: https://www.oecd.org/edu/imhe/QT%20policies%20and%20practices.pdf (Accessed: 3 January 2018).

Henseler, H. and Loenhout, S. van (2018) ‘Educating judges, prosecutors and lawyers in the use of digital forensic experts’, *Digital Investigation*, 24, pp. S76–S82. doi: 10.1016/j.diin.2018.01.010.

HESA (no date) *Rounding and suppression to anonymise statistics | HESA*. Available at: https://www.hesa.ac.uk/about/regulation/data-protection/rounding-and-suppression-anonymise-statistics (Accessed: 30 June 2017).

Higher Education Academy (2019) *UK Engagement Survey*, *Higher Education Academy*. Available at: https://www.heacademy.ac.uk/institutions/surveys/uk-engagement-survey (Accessed: 19 October 2019).

Higher Education Statistics Agency (HESA) (2017) *Introduction - Students 2015/16*. Available at: https://www.hesa.ac.uk/data-and-analysis/publications/students-2015-16/introduction (Accessed: 13 April 2017).

Higher Education Statistics Agency (HESA) (2019) *Graduate Outcomes Survey*, *HESA*. Available at: https://www.graduateoutcomes.ac.uk/ (Accessed: 19 October 2019).

Home Office (2010) *Cyber Crime strategy*. Norwich: The Stationery Office (CM 7842). Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf (Accessed: 4 March 2018).

Horsman, G. (2019) 'Tool testing and reliability issues in the field of digital forensics', *Digital Investigation*, 28, pp. 163–175. doi: 10.1016/j.diin.2019.01.009.

Hossain, Md. M., Fotouhi, M. and Hasan, R. (2015) 'Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things', in *2015 IEEE World Congress on Services*. *2015 IEEE World Congress on Services (SERVICES)*, New York City, NY, USA: IEEE, pp. 21–28. doi: 10.1109/SERVICES.2015.12.

Huebner, E., Bem, D. and Cheung, H. (2010) 'Computer Forensics Education – the Open Source Approach', in Huebner, E. and Zanero, S. (eds) *Open Source Software for Digital Forensics*. Boston, MA: Springer US, pp. 9–23. Available at: http://link.springer.com/10.1007/978-1-4419-5803-7_2 (Accessed: 31 March 2015).

IBM Knowledge Center (2014a) *Categorical Principal Components Analysis (CATPCA)*, *IBM Knowledge Center*. Available at: https://www.ibm.com/support/knowledgecenter/en/SSLVMB_22.0.0/com.ibm.spss.statistics.help/spss/categories/idh_cpca.htm#idh_cpca (Accessed: 25 May 2018).

IBM Knowledge Center (2014b) *KMO and Bartlett's Test*, *IBM Knowledge Center*. Available at: https://www.ibm.com/support/knowledgecenter/en/SSLVMB_24.0.0/spss/tutorials/fac_telco_kmo_01.html (Accessed: 25 May 2018).

Ibrahim, A. M. (2001) 'Differential Responding to Positive and Negative Items: The Case of a Negative Item in a Questionnaire for Course and Faculty Evaluation', *Psychological Reports*, (88), pp. 497–500.

Information Commissioner's Office (2015) *Data Protection Act 1998: Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998*. United Kingdom: Williams Lea Group. Available at: https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf (Accessed: 4 March 2018).

Information Commissioner's Office (2016) 'TalkTalk cyber attack – how the ICO's investigation unfolded', *Information Commissioner's Office (ICO)*. Available at: https://ico.org.uk/about-the-ico/news-and-events/talktalk-cyber-attack-how-the-ico-investigation-unfolded/ (Accessed: 4 March 2018).

Information Commissioner's Office (2017) 'Greater Manchester Police fined after victim interview videos go missing', *Information Commissioner's Office (ICO)*, 4 May. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/05/greater-manchester-police-fined-after-victim-interview-videos-go-missing/ (Accessed: 4 March 2018).

Information Commissioner's Office (2018a) 'Carphone Warehouse fined £400,000 after serious failures placed customer and employee data at risk', *Information Commissioner's Office (ICO)*, 10 January. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/01/carphone-warehouse-fined-400-000-after-serious-failures-placed-customer-and-employee-data-at-risk/ (Accessed: 4 March 2018).

Information Commissioner's Office (2018b) 'Credit reference agency Equifax fined for security breach', *Information Commissioner's Office (ICO)*, 20 September. Available at: https://icoumbraco.azurewebsites.net/about-the-ico/news-and-events/news-and-blogs/2018/09/credit-reference-agency-equifax-fined-for-security-breach/ (Accessed: 24 February 2019).

Information Commissioner's Office (2018c) 'Data security incident trends: What action we've taken in Q4, what you've reported to us and what you can do to stay secure', *Information Commissioner's Office (ICO)*, 14 May. Available at: https://ico.org.uk/action-weve-taken/data-security-incident-trends/ (Accessed: 15 August 2018).

Information Commissioner's Office (2018d) 'Findings, recommendations and actions from ICO investigation into data analytics in political campaigns', *Information Commissioner's Office (ICO)*, 11 July. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/ (Accessed: 15 August 2018).

Information Commissioner's Office (2018e) 'ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information', *Information Commissioner's Office (ICO)*, 25 October. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/ (Accessed: 24 February 2019).

Information Commissioner's Office (ICO) (2018) *Yahoo! fined £250,000 after systemic failures put customer data at risk*, *ICO*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/06/yahoo-fined-250-000-after-systemic-failures-put-customer-data-at-risk/ (Accessed: 2 September 2018).

Institute of Chartered Accountants in England and Wales (2018) *Audit insights: cyber security coping with increasing complexity*. London: ICAEW (Audit Insights). Available at: https://www.icaew.com/-/media/corporate/files/technical/audit-and-assurance/audit-insights/audit-insights-cyber-security-coping-with-increasing-complexity.ashx (Accessed: 14 January 2019).

International Bureau of Education (2017) *Training Tools for Curriculum Development: Developing and Implementing Curriculum Frameworks*. IBE/2017/OP/CD/02. Geneva: United Nations Educational, Scientific and Cultural Organization. Available at: http://unesdoc.unesco.org/images/0025/002500/250052e.pdf (Accessed: 9 August 2018).

International Organization for Standardization (2015) *ISO/IEC 30121:2015(en), Information technology — Governance of digital forensic risk framework*. Standards ISO/IEC 30121:2015(en). International Organization for Standardization (ISO). Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:30121:ed-1:v1:en (Accessed: 25 June 2020).

International Organization for Standardization (2015b) 'ISO/IEC 27043:2015, Information technology — Security techniques — Incident investigation principles and processes'. International Organization for Standardization (ISO). Available at: https://www.iso.org/obp/ui/#iso:std:44407:en (Accessed: 30 January 2019).

International Organization for Standardization (ISO) (no date) *About ISO*, *International Organization for Standardization (ISO)*. Available at: http://www.iso.org/cms/render/live/en/sites/isoorg/home/about-us.html (Accessed: 9 February 2019).

International Organization for Standardization (ISO) (2012) *ISO/IEC 27032:2012, Information technology — Security techniques — Guidelines for cybersecurity*. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en (Accessed: 9 February 2019).

International Organization for Standardization (ISO) (2017) *ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories*. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:17025:ed-3:v1:en (Accessed: 30 January 2019).

International Organization for Standardization (ISO) (2018) *ISO/IEC 27000:2018, Information technology — Security techniques - Information security management systems - Overview and vocabulary*. Available at: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip.

Irish Data Protection Commission (2018) 'Facebook Data Breach - Commencement of Investigation', *Data Protection Commission (DPC)*. Online, 3 October. Available at: https://www.dataprotection.ie/news-media/press-releases/facebook-data-breach-commencement-investigation (Accessed: 24 February 2019).

Irons, A. (no date) 'Problem Based Learning (PBL) in Cybersecurity'. *Higher Education Academy*, University of Gloucester. Available at: https://www.heacademy.ac.uk/download/problem-based-learning-pbl-cyber-security.

Irons, A. and Konstadopoulou, A. (2014) 'Professionalism in digital forensics', *Digital Evidence and Electronic Signature Law Review*, 4(0). doi: 10.14296/deeslr.v4i0.1798.

Irons, A. and Lallie, H. (2014) 'Digital Forensics to Intelligent Forensics', *Future Internet*, 6(3), pp. 584–596. doi: 10.3390/fi6030584.

Irons, A., Stephens, P. and Ferguson, R. (2009) 'Digital Investigation as a distinct discipline: a pedagogic perspective', *Digital Investigation*, 6(1), pp. 82–90. doi: 10.1016/j.diin.2009.05.002.

Irons, A. and Thomas, P. (2014) 'Problem Based Learning in Digital Forensics', *Innovation in Teaching and Learning in Information and Computer Sciences*, pp. 1–10. doi: 10.11120/ital.2014.00013.

Irons, A. and Thomas, P. (2016) 'Problem based learning in digital forensics', *Higher Education Pedagogies*, 1(1), pp. 95–105. doi: 10.1080/23752696.2015.1134200.

ISO (no date) *ISO/IEC JTC 1/SC 27 - IT Security techniques*, *International Organization for Standardization (ISO)*. Available at: https://www.iso.org/committee/45306/x/catalogue/p/1/u/0/w/0/d/0 (Accessed: 30 January 2019).

ISO (1989) *ISO/IEC JTC 1/SC 27 - IT Security techniques*, *International Organization for Standardization (ISO)*. Available at: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/committee/04/53/45306.html (Accessed: 30 January 2019).

ISO (2012a) 'ISO/IEC 27037:2012, Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence'. International Organization for Standardization (ISO). Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en (Accessed: 30 January 2019).

ISO (2012b) *ISO/TC 272 - Forensic sciences, International Organization for Standardization (ISO)*. Available at: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/committee/43/95/4395817.html (Accessed: 30 January 2019).

ISO (2015a) 'ISO/IEC 27042:2015, Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence'. International Organization for Standardization (ISO). Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en (Accessed: 30 January 2019).

James, J. and Gladyshev, P. (2013a) 'A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview', *Digital Investigation*, 10(2), pp. 148–157. doi: 10.1016/j.diin.2013.04.005.

James, J. and Gladyshev, P. (2013b) 'Challenges with Automation in Digital Forensic Investigations', *arXiv preprint arXiv:1303.4498*. Available at: http://arxiv.org/abs/1303.4498 (Accessed: 28 December 2015).

Jick, T. D. (1979) 'Mixing Qualitative and Quantitative Methods: Triangulation in Action', *Administrative Science Quarterly*, 24(4), pp. 602–611. doi: 10.2307/2392366.

Joint Committee on the National Security Strategy (2018) *Cyber Security of the UK's Critical National Infrastructure*. 3rd. London: Authority of the House of Lords and House of Commons, p. 64. Available at: https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf.

Joint Task Force on Cybersecurity Education (2017) 'Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity', in. (Computing Curricula Series). doi: 10.1145/3184594.

Jolliffe, I. T. (2002) *Principal Component Analysis*. 2nd edn. New York: Springer-Verlag. Available at: http://cda.psych.uiuc.edu/statistical_learning_course/Jolliffe%20I.%20Principal%20Component%20Analysis%20(2ed.,%20Springer,%202002)(518s)_MVsa_.pdf (Accessed: 8 August 2018).

Jones, N. (2004) 'Training and accreditatione who are the experts?', *Digital Investigation*, 1(3), pp. 189–194. doi: 10.1016/j.diin.2004.07.009.

Kaminska, O. and Foulsham, T. (2013) 'Understanding sources of social desirability bias in different modes: evidence from eye-tracking', (No. 2013-04). Available at: https://www.iser.essex.ac.uk/research/publications/working-papers/iser/2013-04.pdf (Accessed: 6 September 2018).

Kandiko, C. B. and Mawer, M. (2013) *Student Expectations and Perceptions of Higher Education*. London: King's College London. Available at: https://www.kcl.ac.uk/study/learningteaching/kli/People/Research/DL/QAAReport.pdf (Accessed: 1 May 2017).

Kanellis, P., Kiountouzis, E. and Kolokotronis, N. (2006) *Digital Crime and Forensic Science in Cyberspace*. Idea Group Inc (IGI).

Kaplan, D. (ed.) (2004) *The Sage handbook of quantitative methodology for the social sciences*. Thousand Oaks, California: SAGE Publications, Inc. Available at: https://www.researchgate.net/profile/Nguyen_Trung_Hiep_3/post/Please_mention_a_good_text_book_of_Research_Methodology_in_Social_Science/attachment/59d62ca279197b807798af47/AS:347545596383

234@1459872735672/download/The+SAGE+Handbook+of+Quantitative+Methodology+for+the+Social+Sciences.pdf#page=64.

Kapp, K. M. (2012) *The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education*. San Francisco, CA: John Wiley & Sons.

Karabiyik, U. (2015) *Building an Intelligent Assistant for Digital Forensics*. Florida State University. Available at: https://pdfs.semanticscholar.org/5350/676fae09092b42731448acae3469cba8919c.pdf (Accessed: 1 January 2019).

Karamizadeh, S. *et al.* (2013) 'An Overview of Principal Component Analysis', *Journal of Signal and Information Processing*, 04(03), pp. 173–175. doi: 10.4236/jsip.2013.43B031.

Karie, N. M. and Venter, H. S. (2014) 'Toward a General Ontology for Digital Forensic Disciplines', *Journal of Forensic Sciences*, 59(5), pp. 1231–1241. doi: 10.1111/1556-4029.12511.

Karie, N. M. and Venter, H. S. (2015) 'Taxonomy of Challenges for Digital Forensics', *Journal of Forensic Sciences*, 60(4), pp. 885–893. doi: 10.1111/1556-4029.12809.

Kay, J. *et al.* (2000) 'Problem-Based Learning for Foundation Computer Science Courses', *Computer Science Education*, 10(2), pp. 109–128. doi: 10.1076/0899-3408(200008)10:2;1-C;FT109.

Kemp, S. (2017) 'Digital in 2017: Global Overview', *We Are Social*, 24 January. Available at: https://wearesocial.com/special-reports/digital-in-2017-global-overview (Accessed: 22 February 2019).

Kemp, S. (2019) 'Digital 2019: Global Internet Use Accelerates', *We Are Social*, 30 January. Available at: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates (Accessed: 22 February 2019).

Kennedy, S. D. (2016) 'Your Password Has Expired and Must Be Changed', *Information Today*, 33(3). Available at: http://infotoday.com/it/apr16/Kennedy--Your-Password-Has-Expired-and-Must-Be-Changed.shtml (Accessed: 22 February 2019).

Kessler, G. (2007) 'Online education in computer and digital forensics: A case study', in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*. IEEE, pp. 264a–264a. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4076915 (Accessed: 9 April 2015).

Kessler, G. C., Simpson, R. and Fry, J. (2009) 'Multidisciplinary learning using mock trials', *International Journal of Electronic Security and Digital Forensics*, 2(2), pp. 141–155.

Kessler, G. and Ramsay, J. (2014) 'A Proposed Curriculum in Cybersecurity Education Targeting Homeland Security Students', in. IEEE, pp. 4932–4937. doi: 10.1109/HICSS.2014.605.

Kessler, G. and Schirling, M. (2006) 'The design of an undergraduate degree program in computer & digital forensics', *Journal of Digital Forensics, Security and Law*, 1(3), pp. 37–50.

Kinnunen, P. *et al.* (2018) 'Understanding initial undergraduate expectations and identity in computing studies', *European Journal of Engineering Education*, 43(2), pp. 201–218. doi: 10.1080/03043797.2016.1146233.

Kiper, R. (2017) *Forensication Education: Towards a Digital Forensics Instructional Framework*. US: SANS Institute. Available at: https://www.sans.org/reading-room/whitepapers/forensics/forensication-education-digital-forensics-instructional-framework-37582 (Accessed: 10 May 2017).

Kirkpatrick, D. and Kirkpatrick, J. D. (2006) *Evaluating Training Programs: The Four Levels*. 3rd edn. San Francisco, California: Berrett-Koehler Publishers.

Knörl, S. *et al.* (2015) 'Reconstructing students' subjective theories on self-directed learning a qualitative research approach in Software Engineering education', in *2015 IEEE Global Engineering Education Conference (EDUCON). 2015 IEEE Global Engineering Education Conference (EDUCON)*, pp. 314–317. doi: 10.1109/EDUCON.2015.7095990.

Knowles, M. S. (1975) *Self-directed Learning: A Guide for Learners and Teachers*. London: Cambridge Adult Education.

Knox, B. *et al.* (2018) 'Education for Cognitive Agility: Improved Understanding and Governance of Cyberpower', in *European Conference on Cyber Warfare and Security*. Oslo, Norway: Academic Conferences International Limited, pp. 541–550. Available at: https://www.researchgate.net/profile/Stefan_Suetterlin/publication/331021729_Education_for_Cognitive_Agility_Improved_Understanding_and_Governance_of_Cyberpower/links/5c6189b4a6fdccb608b8d40e/Education-for-Cognitive-Agility-Improved-Understanding-and-Governance-of-Cyberpower.pdf.

Könings, K. D., Brand-Gruwel, S. and Merriënboer, J. J. G. V. (2005) 'Towards more powerful learning environments through combining the perspectives of designers, teachers, and students.', *The British journal of educational psychology*, 75(Pt 4), pp. 645–660. doi: 10.1348/000709905x43616.

Kortjan, N. and Solms, R. von (2014) 'A conceptual framework for cyber security awareness and education in SA', *South African Computer Journal*, 52. doi: 10.18489/sacj.v52i0.201.

Krakoff, S. (no date) 'What's the Difference Between Cybersecurity and Computer Forensics?', *Champlain College Online*. Available at: https://4a2fd7f23d864318bc3a28e8a2b1590e.pages.ubembed.com/3c4f074e-b8d9-4721-a5e2-c2b2e3945e6f/c.html?closedAt=0 (Accessed: 30 December 2018).

Krishman, Dr. A. (2009) *What are Academic Disciplines? Some observations on the Disciplinarity vs. Interdisciplinarity debate*. University of Southampton: ESRC National Centre of Research Methods. Available at: http://eprints.ncrm.ac.uk/783/1/what_are_academic_disciplines.pdf (Accessed: 7 September 2017).

Kyriacou, C. and Stephens, P. (1999) 'Student Teachers' Concerns During Teaching Practice', *Evaluation & Research in Education*, 13(1), pp. 18–31. doi: 10.1080/09500799908666943.

Lallie, H. S. (2010) 'The Use of Digital Forensic Case Studies for Teaching and Assessment', *Cybercrime Forensics Education and Training*, pp. 1–9.

Lallie, H. S., Lawson, P. and Day, D. (2011) 'Using digital logs to reduce academic misdemeanour by students in digital forensic assessments', *Journal of Information Technology Education*, 10, pp. 255–269.

Lallie, M. H. S. and Day, D. J. (2012) 'Industrial engagement in information security and digital forensics: achieving the transitional blend from academia to industry', in. *HEA Stem Conference*, Imperial College, London: Higher Education Academy.

Lang, A. *et al.* (2014) 'Developing a new digital forensics curriculum', *Digital Investigation*, 11, pp. S76–S84. doi: 10.1016/j.diin.2014.05.008.

LastPass (2018) *Psychology of Passwords: Neglect is Helping Hackers Win*. LogMeIn. Available at: https://m.softchoice.com/web/newsite/documents/amplify/LogMeIn-Software-The-Psychology-of-Passwords.pdf (Accessed: 22 February 2019).

Lavrakas, P. J. (2008) *Encyclopedia of Survey Research Methods* (2 vol). Thousand Oaks, CA: SAGE Publications. Available at: https://books.google.co.uk/books?id=2sr0CAAAQBAJ&printsec=frontcover.

Lee, D. (2018) 'Up to 50m Facebook accounts attacked', *BBC News*. Online, 29 September. Available at: https://www.bbc.com/news/technology-45686890 (Accessed: 24 February 2019).

Leeuw, E. D. de *et al.* (2008) *International Handbook of Survey Methodology*. Taylor & Francis.

Leyden, J. (2005) 'UK Uni launches computer forensics course', *The Register*, 30 June. Available at: https://www.theregister.co.uk/2005/06/30/computer_forensics_degree/ (Accessed: 19 March 2017).

Leyden, J. (2013) *Crap security lands Sony £250k fine for PlayStation Network hack*. Available at: https://www.theregister.co.uk/2013/01/24/sony_psn_breach_fine/ (Accessed: 12 April 2015).

Lillis, D., O'Sullivan, T. and Scanlon, M. (2016) 'Current Challenges and Future Research Areas for Digital Forensic Investigation', in. *The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)*, Daytona Beach, FL, USA: Association of Digital Forensics, Security and Law (ADFSL), pp. 9–20. Available at: https://markscanlon.co/papers/CurrentChallengesAndFutureResearchAreas.pdf (Accessed: 5 January 2018).

Linting, M. *et al.* (2007) 'Nonlinear principal components analysis: Introduction and application.', *Psychological Methods*, 12(3), pp. 336–358. doi: 10.1037/1082-989X.12.3.336.

Linting, M. and van der Kooij, A. (2011) 'Nonlinear Principal Components Analysis With CATPCA: A Tutorial', *Journal of Personality Assessment*, 94(1), pp. 12–25. doi: 10.1080/00223891.2011.627965.

Littlewood, S. *et al.* (2005) 'Early practical experience and the social responsiveness of clinical education: systematic review', *BMJ : British Medical Journal*, 331(7513), pp. 387–391.

Liu, J. (2016) 'Baccalaureate programs in computer forensics', in *2016 IEEE International Conference on Electro Information Technology (EIT). 2016 IEEE International Conference on Electro Information Technology (EIT)*, Grand Forks, ND, USA: IEEE, pp. 0615–0620. doi: 10.1109/EIT.2016.7535309.

Lowden, K. *et al.* (2011) 'Employers' perceptions of the employability skills of new graduates', *London: Edge Foundation*.

Luhanga, F. L., Larocque, S. and MacEwan, L. (2014) 'Exploring the Issue of Failure to Fail in Professional Education Programs: A Multidisciplinary Study', *Journal of University Teaching & Learning Practice*, 11(2), p. 26.

Luiijf, E., Besseling, K. and De Graaf, P. (2013) 'Nineteen national cyber security strategies', *International Journal of Critical Infrastructures*, 9(1–2), pp. 3–31. doi: 10.1504/IJCIS.2013.051608.

Macaulay, T. (2018) ‘The biggest ICO fines for data protection breaches’, *ComputerworldUK*, 27 November. Available at: https://www.computerworlduk.com/galleries/data/biggest-fines-issued-by-ico-3679087/ (Accessed: 24 February 2019).

MacDermott, A., Baker, T. and Shi, Q. (2018) ‘Iot Forensics: Challenges for the Ioa Era’, in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris: IEEE, pp. 1–5. doi: 10.1109/NTMS.2018.8328748.

Maguire, M. and Delahunt, B. (2017) ‘Doing a Thematic Analysis: A Practical, Step-by-Step Guide for Learning and Teaching Scholars’, *AISHE-J: The All Ireland Journal of Teaching and Learning in Higher Education*, 8(3), pp. 3351–33514.

McMillan, J. E. R., Glisson, W. B. and Bromby, M. (2013) ‘Investigating the Increase in Mobile Phone Evidence in Criminal Activities’, in *2013 46th Hawaii International Conference on System Sciences*. *2013 46th Hawaii International Conference on System Sciences*, pp. 4900–4909. doi: 10.1109/HICSS.2013.366.

Meister, S. and Chassanoff, A. (2014) ‘Integrating Digital Forensics Techniques into Curatorial Tasks: A Case Study’, *International Journal of Digital Curation*, 9(2). doi: 10.2218/ijdc.v9i2.325.

Metropolitan Police Procurement Services (2015) *MPS - Digital, Cyber and Communications Forensics Unit Information for Prospective Bidders*. 4.4. Available at: https://www.bluelight.gov.uk/procontract/attachment_26.nsf/dsp_frm_attachments/ATT-9ZCB-TXKJU7/$FILE/Memorandum%20of%20Information%20v1%2020150715.pdf (Accessed: 19 October 2015).

Meyers, M. and Rogers, M. (2004) ‘Computer forensics: the need for standardization and certification’, *International Journal of Digital Evidence*, 3(2), pp. 1–11.

Miranda Lopez, E., Moon, S. and Park, J. (2016) ‘Scenario-Based Digital Forensics Challenges in Cloud Computing’, *Symmetry*, 8(10), p. 107. doi: 10.3390/sym8100107.

Mislan, R. P., Casey, E. and Kessler, G. C. (2010) ‘The growing need for on-scene triage of mobile devices’, *Digital Investigation*, 6(3–4), pp. 112–124. doi: 10.1016/j.diin.2010.03.001.

Mitchell, F. (2014) ‘The use of Artificial Intelligence in digital forensics: An introduction’, *Digital Evidence and Electronic Signature Law Review*, 7(0). doi: 10.14296/deeslr.v7i0.1922.

Moch, C. and Freiling, F. C. (2009) ‘The Forensic Image Generator Generator (Forensig2)’, in *2009 Fifth International Conference on IT Security Incident Management and IT Forensics*. *2009 Fifth International Conference on IT Security Incident Management and IT Forensics*, pp. 78–93. doi: 10.1109/IMF.2009.8.

Monahan, T. and Fisher, J. A. (2010) ‘Benefits of “Observer Effects”: Lessons from the Field’, *Qualitative research : QR*, 10(3), pp. 357–376. doi: 10.1177/1468794110362874.

Montasari, R. and Hill, R. (2019) ‘Next-Generation Digital Forensics: Challenges and Future Paradigms’, in *12th International Conference on Global Security, Safety and Sustainability (ICGS3)*. *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, London: IEEE, pp. 205–212. doi: 10.1109/ICGS3.2019.8688020.

Moore, T. (2006) ‘The Economics of Digital Forensics’, in *Fifth Workshop on the Economics of Information Security*. *WEIS*. Available at:

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.130.9969&rep=rep1&type=pdf (Accessed: 1 January 2015).

Muntean, C. (2011) ‘Raising engagement in e-learning through gamification’, in *Proc. 6th International Conference on Virtual Learning ICVL*. Romania, pp. 323–329. Available at: http://icvl.eu/2011/disc/icvl/documente/pdf/met/ICVL_ModelsAndMethodologies_paper42.pdf (Accessed: 6 January 2016).

Nagarajan, A. *et al.* (2012) ‘Exploring game design for cybersecurity training’, in *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on*. IEEE, pp. 256–262. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6392562 (Accessed: 10 April 2015).

Nance, K., Armstrong, H. and Armstrong, C. (2010) ‘Digital Forensics: Defining an Education Agenda’, in *2010 43rd Hawaii International Conference on System Sciences (HICSS)*. *2010 43rd Hawaii International Conference on System Sciences (HICSS)*, pp. 1–10. doi: 10.1109/HICSS.2010.151.

National Crime Agency (no date) *Cyber crime: Preventing young people from getting involved in cyber crime*, *National Crime Agency*. Available at: http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved (Accessed: 22 February 2019).

National Crime Agency (2016) *Cyber Crime Assessment 2016: Need for a stronger law enforcement and business partnership to fight cyber crime*. 1.2. London, United Kingdom: Strategic Cyber Industry Group (SCIG). Available at: http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file (Accessed: 17 February 2018).

National Institute of Justice (2016) *The Computer Forensics Reference Data Sets Project*, *NIST CFReDS*. Available at: https://www.cfreds.nist.gov/ (Accessed: 10 May 2017).

NCSC (2016) *Certification Master’s Degrees in Digital Forensics Call for Applications*. 3.0. United Kingdom: GCHQ. Available at: https://www.ncsc.gov.uk/content/files/protected_files/article_files/Certification-Masters-DF-Issue-3-0-01September2016.pdf (Accessed: 15 September 2016).

NCSC (2017a) *Certification Master’s Degrees in Digital Forensics Call for Applications*. 4.0. United Kingdom: GCHQ. Available at: https://www.ncsc.gov.uk/content/files/protected_files/article_files/Certification-Masters-Digital-Forensics-Issue-4-0-01August2017.pdf (Accessed: 3 August 2017).

NCSC (2017b) *Certification of Bachelor’s Degrees in Computer Science and Digital Forensics*. Standards 2.0. United Kingdom: National Cyber Security Centre. Available at: https://www.ncsc.gov.uk/content/files/protected_files/article_files/Certification-Bachelors-2_0-20171214.pdf (Accessed: 1 January 2018).

NCSC (2018a) *NCSC degree certification - Call for new applicants*. Available at: https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0 (Accessed: 17 August 2018).

NCSC (2018b) *NCSC-certified degrees*. Available at: https://www.ncsc.gov.uk/information/ncsc-certified-degrees (Accessed: 17 August 2018).

NCSC (2019) *NCSC degree certification - Call for new applicants*, *National Cyber Security Centre*. Available at: https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0 (Accessed: 20 February 2019).

Newhouse, W. *et al.* (2017) *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. NIST SP 800-181. Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.SP.800-181.

Nogala, D. *et al.* (eds) (2016) 'European Police Science and Research Bulletin', in *Global trends in law enforcement training and education*. *CEPOL European Police Research and Science Conference*, Budapest, Hungary: European Union Agency for Law Enforcement Training (CEPOL (Special Conference Edition), p. 276. doi: 10.2825/13491.

Nordhaug, Ø. A. (2013) *The Forensic Challenger-A Digital Forensic E-Learning Platform*. phdthesis. Gjøvik University College. Available at: http://brage.bibsys.no/xmlui/handle/11250/198683 (Accessed: 6 January 2016).

Norman, G. (2008) 'Problem-based learning makes a difference. But why?', *CMAJ : Canadian Medical Association Journal*, 178(1), pp. 61–62. doi: 10.1503/cmaj.071590.

Norman, J. and Williams, E. (2016) 'Putting Learning into practice: self-reflections from cops', in *European Police Science and Research Bulletin*. Budapest, Hungary: European Union Agency for Law Enforcement Training (CEPOL (Special Conference Edition, 3), pp. 197–204. Available at: https://bulletin.cepol.europa.eu/index.php/bulletin/issue/view/23/European%20Police%20Science%20and%20Research%20Bulletin%20-%20Special%20Conference%20Edition%20n.%203 (Accessed: 15 August 2018).

Office of Inspector General (2015) *DHS Can Strengthen Its Cyber Mission Coordination Efforts*. OIG-15-140. Washington, DC: Department of Homeland Security. Available at: https://www.hsdl.org/?view&did=787220 (Accessed: 25 January 2019).

Olivier, M. S. (2009) 'On metadata context in Database Forensics', *Digital Investigation*, 5(3–4), pp. 115–123. doi: 10.1016/j.diin.2008.10.001.

Omar, T., Venkatesan, S. and Amamra, A. (2018) 'Development of Undergraduate Interdisciplinary Cybersecurity Program: A Literature Survey', in. *2018 ASEE Annual Conference & Exposition*, Salt Lake City, UT: American Society for Engineering Education. Available at: https://www.asee.org/public/conferences/106/papers/22996/view (Accessed: 9 February 2019).

Onwuegbuzie, A. J. and Frels, R. (2016) *Seven Steps to a Comprehensive Literature Review: A Multimodal and Cultural Approach*. SAGE.

Oxford University Press (2004) 'omission, n.', *OED Online*. 3rd edn. Oxford: Oxford University Press. Available at: http://www.oed.com/view/Entry/131211 (Accessed: 16 February 2019).

Oxford University Press (2011) 'framework, n.', *OED Online*. 3rd edn. Oxford: Oxford University Press. Available at: http://www.oed.com/view/Entry/74161 (Accessed: 19 February 2019).

Oxford University Press (2014) 'workshop, n.', *OED Online*. 3rd edn. Oxford: Oxford University Press. Available at: http://www.oed.com/view/Entry/230253 (Accessed: 8 August 2018).

Oxford University Press (2015) *Definition of science in English*. Available at: http://www.oxforddictionaries.com/definition/english/science (Accessed: 17 June 2015).

Pan, Y. *et al.* (2012) 'Game-based Forensics Course For First Year Students', in *Proceedings of the 13th annual conference on Information technology education. Annual conference on Information technology education*, Calgary, AB, Canada: ACM, pp. 13–18.

Pan, Y., Schwartz, D. and Mishra, S. (2015) 'Gamified digital forensics course modules for undergraduates', in. IEEE, pp. 100–105. doi: 10.1109/ISECon.2015.7119899.

Parr, C. (2014) 'First GCHQ-certified master's courses unveiled', *Times Higher Education (THE)*, 1 August. Available at: https://www.timeshighereducation.com/news/first-gchq-certified-masters-courses-unveiled/2014921.article (Accessed: 17 August 2018).

Parsonage, H. (2009) *Computer Forensics Case Assessment And Triage - Some Ideas for Discussion*. Available at: http://computerforensics.parsonage.co.uk/triage/ComputerForensicsCaseAssessmentAndTriageDiscussionPaper.pdf (Accessed: 21 December 2015).

Parsons, J. *et al.* (2013) *Engaging in Action Research: A Practical Guide to Teacher-Conducted Research for Educators and School Leaders*. Brush Education.

Parsons, K. *et al.* (2017) 'The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies', *Computers & Security*, 66, pp. 40–51. doi: 10.1016/j.cose.2017.01.004.

Patton, M. Q. (2002) 'Qualitative Evaluation Checklist'. Western Michigan University The Evaluation Center. Available at: https://wmich.edu/sites/default/files/attachments/u350/2018/qual-eval-patton.pdf (Accessed: 20 February 2019).

Pérez, L. C. *et al.* (2011) 'Information assurance education in two- and four-year institutions', in *Proceedings of the 16th annual conference reports on Innovation and technology in computer science education - working group reports - ITiCSE-WGR '11. the 16th annual conference reports*, Darmstadt, Germany: ACM Press, p. 39. doi: 10.1145/2078856.2078860.

Potter, L. E. and Vickers, G. (2015) 'What Skills do you Need to Work in Cyber Security?: A Look at the Australian Market', in *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research - SIGMIS-CPR '15. the 2015 ACM SIGMIS Conference*, Newport Beach, California, USA: ACM Press, pp. 67–72. doi: 10.1145/2751957.2751967.

PricewaterhouseCoopers (PwC) (2017) *Privacy and Security Enforcement Tracker 2016*. Annual Report. United Kingdom: PricewaterhouseCoopers LLP. Available at: https://www.pwc.co.uk/press-room/assets/privacy-and-security-enforcement-tracker-2016.pdf (Accessed: 4 March 2018).

Pringle, J. and Potter, J. (2014) 'Educational e-gaming to provide an innovative, effective and flexible 24/7 learning environment'. Available at: https://www.heacademy.ac.uk/sites/default/files/GEES-004-O.pptx (Accessed: 15 April 2015).

Punch, K. F. (2005) *Introduction to Social Research: Quantitative and Qualitative Approaches*. SAGE.

Pusey, P., Gondree, M. and Peterson, Z. (2016) 'The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations', *IEEE Security & Privacy*, 14(6), pp. 90–95. doi: 10.1109/MSP.2016.119.

Qasem, M. A. N. and Gul, S. B. A. (2014) 'Effect of Items Direction (Positive or Negative) on the Factorial Construction and Criterion related Validity in Likert Scale', *Khazar Journal of Humanities and Social Sciences*, 17(3), pp. 77–84.

Ramirez, R. B. (2017) *Making Cyber Security Interdisciplinary: Recommendations for a Novel Curriculum and Terminology Harmonization*. Master of Science in Technology and Society. Columbia University. Available at: https://dspace.mit.edu/bitstream/handle/1721.1/111232/1003284196-MIT.pdf?sequence=1.

Ravitch, S. M. and Carl, N. M. (2015) *Qualitative Research: Bridging the Conceptual, Theoretical, and Methodological*. United State of America: SAGE Publications, Inc. Available at: https://books.google.co.uk/books?id=V6tiCgAAQBAJ&printsec=frontcover#v=onepage&q&f=false.

Rawlings, P., White, P. and Stephens, R. (2005) 'Practice-Based Learning in Information Systems: The Advantages for Students', *Journal of Information Systems Education*, 16(4), pp. 455–464.

Reith, M., Carr, C. and Gunsch, G. H. (2002a) 'An Examination of Digital Forensic Models', *International Journal of Digital Evidence (IJDE)*, 1(3), pp. 1–12.

Reith, M., Carr, C. and Gunsch, G. H. (2002b) 'An Examination of Digital Forensic Models', *International Journal of Digital Evidence*, 1(3), p. 12.

Rickman, P. (2004) 'Education versus Training', *Philosophy Now*, September, pp. 31–32.

Ritchie, J. *et al.* (2013) *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. SAGE.

Ritchie, J. and Lewis, J. (eds) (2003) *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. SAGE.

Robinson, M. (2015) *Data Sets, Digital Forensics Workbook*. Available at: http://www.digitalforensicsworkbook.com/data-sets/ (Accessed: 10 May 2017).

Rogers, M. K. and Seigfried, K. (2004) 'The future of computer forensics: a needs analysis survey', *Computers & Security*, 23(1), pp. 12–16. doi: 10.1016/j.cose.2004.01.003.

Rossi, P. H., Wright, J. D. and Anderson, A. B. (2013) *Handbook of Survey Research*. Academic Press.

Roussev, V., Quates, C. and Martell, R. (2013) 'Real-time digital forensics and triage', *Digital Investigation*, 10(2), pp. 158–167. doi: 10.1016/j.diin.2013.02.001.

Rowe, B. R. and Gallaher, M. P. (2006) 'Private Sector Cyber Security Investment: An Empirical Analysis', in *The fifth workshop on the economics of information security*. *WEIS06*, University of Cambridge, England. Available at: https://www.econinfosec.org/archive/weis2006/docs/18.pdf (Accessed: 15 April 2019).

Rowe, D. C., Lunt, B. M. and Ekstrom, J. J. (2011) 'The role of cyber-security in information technology education', in. *SIGITE' 11 ACM Special Interest Group for Information Technology Education Conference*, West Point, NY, USA: ACM Press, pp. 113–121. doi: 10.1145/2047594.2047628.

Ryan, D. J. and Shpantzer, G. (no date) 'Legal Aspects of Digital Forensics'. Available at: https://pdfs.semanticscholar.org/c37f/48ef7f411264d89e9ecbce1ececa5b568de4.pdf (Accessed: 6 June 2016).

Sagor, R. (2005) *The Action Research Guidebook: A Four-Step Process for Educators and School Teams*. Corwin Press. Available at: https://books.google.co.uk/books?id=e_diwK8T45cC&printsec=frontcover#v=onepage&q&f=false.

Salkind, N. J. (2006) *Encyclopedia of Measurement and Statistics*. SAGE Publications.

Salt, D. W., Lallie, H. S. and Lawson, P. (2011) 'Studying First Year Forensic Computing: Managing the Student Experience', *Innovation in Teaching and Learning in Information and Computer Sciences*, 10(1), pp. 91–96. doi: 10.11120/ital.2011.10010091.

Saunders, B. *et al.* (2018) 'Saturation in qualitative research: exploring its conceptualization and operationalization', *Quality & Quantity*, 52(4), pp. 1893–1907. doi: 10.1007/s11135-017-0574-8.

Save the Student (2019) *How much does uni cost you PER HOUR?*, *Save the Student*. Available at: https://www.savethestudent.org/uniperhour/ (Accessed: 9 February 2019).

Savery, J. R. and Duffy, T. M. (1995) 'Problem Based Learning: An Instructional Model and Its Constructivist Framework.', in *Constructivist Learning Environments: Case Studies in Instructional Design*. Englewood Cliffs, NJ: Educational Technology Publications, pp. 135–148. Available at: https://pdfs.semanticscholar.org/549c/9ea78fe19aa609a66e84ea0b2ecda5e731bf.pdf (Accessed: 5 May 2015).

Scanlon, M., Du, X. and Lillis, D. (2017) 'EviPlant: An efficient digital forensic challenge creation, manipulation and distribution solution', *Digital Investigation*, 20, pp. S29–S36. doi: 10.1016/j.diin.2017.01.010.

Schatz, D., Bashroush, R. and Wall, J. (2017) 'Towards a More Representative Definition of Cyber Security', *The Journal of Digital Forensics, Security and Law*, 12(2), pp. 53–74. doi: 10.15394/jdfsl.2017.1476.

Scimago Lab (2018) *Scimago Journal & Country Rank*. Available at: https://www.scimagojr.com/ (Accessed: 13 February 2019).

Se, S. and Jasiobedzki, P. (2005) 'Instant Scene Modeler for Crime Scene Reconstruction', in *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05) - Workshops*. *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05) - Workshops*, pp. 123–123. doi: 10.1109/CVPR.2005.477.

Segre, M. (2015) *Higher Education and the Growth of Knowledge: A Historical Outline of Aims and Tensions*. Routledge.

Seidel, J. V. (1998) 'Qualitative Data Analysis'. Qualis Research. Available at: ftp://ftp.qualisresearch.com/pub/qda.pdf (Accessed: 6 July 2018).

Seldon, A. (2017) 'It's time to debunk the myth surrounding two-year degrees', *The Telegraph*. Online, 14 December. Available at: https://www.telegraph.co.uk/education/2017/12/14/time-debunk-myths-surrounding-two-year-degrees/ (Accessed: 6 March 2018).

Select Committee on Science and Technology (2018) 'BSI - Written Evidence: Forensic Science'. House of Lords. Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee-lords/forensic-science/written/94568.pdf (Accessed: 30 January 2019).

Sesay, A. (2012) *Educational Research: A Beginner's Guide*. Xlibris Corporation. Available at: https://books.google.co.uk/books?id=DdpQAAAAQBAJ&printsec=frontcover (Accessed: 30 August 2018).

Shakamuri, M. (2006) 'Forensic Certifications'. Available at: https://www.cs.nmt.edu/df/StudentPapers/Shakamuri_Forensic_Certifications.pdf (Accessed: 15 April 2015).

Shinder, D. L. and Cross, M. (2008) *Scene of the Cybercrime*. 2nd edn. Burlington, MA: Elsevier.

Simmons, O. E. (2010) 'Is That a Real Theory or Did You Just Make It Up? Teaching Classic Grounded Theory | Grounded Theory Review', *Grounded Theory Review: An International Journal*, 9(2). Available at: http://groundedtheoryreview.com/2010/06/25/is-that-a-real-theory-or-did-you-just-make-it-up-teaching-classic-grounded-theory/ (Accessed: 6 July 2018).

Skills for Justice (2010a) *About the Policing Professional Framework (PPF)*. Available at: https://www.skillsforjustice-ppf.com/about/ (Accessed: 2 January 2016).

Skills for Justice (2010b) *Policing Professional Framework (PPF) Hi Tech Crime Unit Manager*. Available at: https://www.skillsforjustice-ppf.com/national-roles/?r_id=106 (Accessed: 2 January 2016).

Skills for Justice (2010c) *Policing Professional Framework (PPF) Hi Tech Investigation Officer*. Available at: http://www.skillsforjustice-ppf.com/national-roles/?rt_id=2&rg_id=9&r_id=108 (Accessed: 2 January 2016).

Skills for Justice (2011) *Policing Professional Framework (PPF) Hi Tech Crime Investigator*. Available at: http://www.skillsforjustice-ppf.com/national-roles/?rt_id=1&rg_id=8&r_id=105 (Accessed: 2 January 2016).

Skills for Justice (2013a) *Policing Professional Framework (PPF) Cyber Infrastructure Officer*. Available at: http://www.skillsforjustice-ppf.com/national-roles/?rt_id=1&rg_id=8&r_id=1092 (Accessed: 2 January 2016).

Skills for Justice (2013b) *Policing Professional Framework (PPF) Cyber Intelligence Analyst*. Available at: http://www.skillsforjustice-ppf.com/national-roles/?rt_id=2&rg_id=9&r_id=1090 (Accessed: 2 January 2016).

Skills for Justice (2013c) *Policing Professional Framework (PPF) Cyber Intelligence Development Officer*. Available at: http://www.skillsforjustice-ppf.com/national-roles/?rt_id=1&rg_id=8&r_id=1089 (Accessed: 2 January 2016).

Skills for Justice (2013d) *Policing Professional Framework (PPF) Cyber Intelligence Researcher*. Available at: http://www.skillsforjustice-ppf.com/national-roles/?rt_id=2&rg_id=9&r_id=1091 (Accessed: 2 January 2016).

Skills for Justice (2013e) *Policing Professional Framework (PPF) Cyber Investigator (DC)*. Available at: http://www.skillsforjustice-ppf.com/national-roles/?rt_id=1&rg_id=8&r_id=1087 (Accessed: 2 January 2016).

Skills for Justice (2013f) *Policing Professional Framework (PPF) Cyber Investigator (DI)*. Available at: https://www.skillsforjustice-ppf.com/national-roles/?r_id=1085 (Accessed: 2 January 2016).

Skills for Justice (2013g) *Policing Professional Framework (PPF) Cyber Investigator (DS)*. Available at: http://www.skillsforjustice-ppf.com/national-roles/?rt_id=1&rg_id=7&r_id=1086 (Accessed: 2 January 2016).

Sobusiak-Fischanaller, M. and Vandermeer, Y. (no date) 'Cybercrime Training Governance Model Cybercrime Training Competency Framework'. Available at: https://rm.coe.int/3148-2-3-ecteg-16-cy-train-module/1680727f34 (Accessed: 25 February 2019).

Solís, M. (2015) 'The dilemma of combining positive and negative items in scales', *Psicothema*, 27(2), pp. 192–200. doi: 10.7334/psicothema2014.266.

Solms, R. von and Niekerk, J. van (2013) 'From information security to cyber security', *Computers & Security*, 38, pp. 97–102. doi: 10.1016/j.cose.2013.04.004.

Sommer, P. (2011) 'Certification, registration and assessment of digital forensic experts: The UK experience', *Digital Investigation*, 8(2), pp. 98–105. doi: 10.1016/j.diin.2011.06.001.

Sommer, P. (2018) 'Accrediting digital forensics: What are the choices?', *Digital Investigation*, 25, pp. 116–120. doi: 10.1016/j.diin.2018.04.004.

Spiekermann, D. *et al.* (2017) 'Challenges of Network Forensic Investigation in Virtual Networks', *Journal of Cyber Security and Mobility*, 5(2), pp. 15–46. doi: 10.13052/jcsm2245-1439.522.

Stambaugh, H. *et al.* (2001) *Electronic Crime Needs Assessment for State and Local Law Enforcement*. U.S. Department of Justice.

Stephens, P. (2012) 'An Evaluation of Linux Cybercrime Forensics Courses for European Law Enforcement', in Clarke, N. and Furnell, S. (eds) *Proceedings of the Sixth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2012)*. Plymouth University, pp. 119–128.

Stephens, P. and Humphries, G. (2014) 'Resourcing computer forensics courses'. University of Sunderland, Sunderland, UK. Available at: http://create.canterbury.ac.uk/12947/ (Accessed: 5 January 2016).

Stephens, P. and Induruwa, A. (2007) 'Cybercrime Investigation Training and Specialist Education for the European Union', in *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007)*. *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007)*, pp. 28–37. doi: 10.1109/WDFIA.2007.4299370.

Strzempka, K. (2010) 'Forensics master's curriculum'. Available at: http://docs.lib.purdue.edu/dissertations/AAI1479951/ (Accessed: 21 January 2016).

The Court Jester (2017) 'Forcing digital forensics to obey "one size fits all" crime lab standard is "stupid and expensive"', 8 June. Available at: https://forums.theregister.co.uk/forum/1/2017/06/08/digital_forensics_standards_push/ (Accessed: 6 November 2018).

The Forensic Science Regulator (2016) *Method Validation in Digital Forensics*. Birmingham, UK: The Forensic Science Regulator (1). Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/528123/FSR_Method_Validation_in_Digital_Forensics_FSR-G-218_Issue_1.pdf (Accessed: 15 May 2017).

The Higher Education Academy (2014) *Professional Placements*. York: The Higher Education Academy. Available at: https://www.heacademy.ac.uk/system/files/resources/professional_placements.pdf (Accessed: 13 February 2018).

The Institute of Information Security Professionals (2018) *IISP Skills Framework*. 2.2. London: The Institute of Information Security Professionals (IISP). Available at: https://www.iisp.org/iisp/About_Us/Our_Skills_Framework/ (Accessed: 27 September 2018).

The Office for National Statistics (2017) *Is pay higher in the public or private sector?*, *Office for National Statistics*. Available at: https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/articles/ispayhigherinthepublicorprivatesector/2017-11-16 (Accessed: 20 November 2019).

The Office for National Statistics (2018a) *Crime in England and Wales: Additional tables on Fraud and Cyber crime*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables (Accessed: 17 February 2018).

The Office for National Statistics (2018b) *Crime in England and Wales: year ending September 2017*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2017 (Accessed: 17 February 2018).

The Office for National Statistics (2018c) *Overview of fraud and computer misuse statistics for England and Wales*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25#what-is-known-about-the-nature-and-circumstances-of-fraud-and-computer-misuse (Accessed: 17 February 2018).

The Office for National Statistics (2018d) *User Guide to Crime Statistics for England and Wales*. London, United Kingdom. Available at: https://www.ons.gov.uk/file?uri=/peoplepopulationandcommunity/crimeandjustice/methodologies/crimeandjusticemethodology/userguidetocrimestatistics.pdf (Accessed: 17 February 2018).

The Quality Assurance Agency for Higher Education (2007) *Computing Subject Benchmark Statement*. Available at: http://www.qaa.ac.uk/en/Publications/Documents/Subject-benchmark-statement-Computing.aspx.pdf (Accessed: 22 April 2015).

The Quality Assurance Agency for Higher Education (2016) *QAA Subject Benchmark Statement - Computing*. Gloucester, United Kingdom: The Quality Assurance Agency. Available at: http://centaur.reading.ac.uk/69459/ (Accessed: 9 May 2017).

The Science and Technology Committee (2005) *Forensic Science on Trial: Seventh Report of Session 2004-05*. 7. London: House of Commons. Available at: https://publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96i.pdf (Accessed: 30 January 2019).

The Stationery Office (2017) *Investigatory Powers Act 2016*. Available at: http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf (Accessed: 22 February 2018).

The Stationery Office Limited (2010) *The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010*, *STATUTORY INSTRUMENTS*. Available at: http://www.legislation.gov.uk/uksi/2010/31/pdfs/uksi_20100031_en.pdf (Accessed: 4 March 2018).

The Student Room (2000) *First Year of Uni Vs. A-Levels... Harder or easier?*, *The Student Room*. Available at: https://www.thestudentroom.co.uk/showthread.php?t=1285791&utm_source=facebook&utm_medium=fblikebutton&utm_campaign=thread (Accessed: 10 June 2016).

The Student Room (2013) *2 year or a 3 year degree*, *The Student Room*. Available at: https://www.thestudentroom.co.uk/showthread.php?t=2305883&utm_source=facebook&utm_medium=fblikebutton&utm_campaign=thread (Accessed: 6 August 2016).

Thomas, D. R. (2006) 'A General Inductive Approach for Analyzing Qualitative Evaluation Data', *American Journal of Evaluation*, 27(2), pp. 237–246. doi: 10.1177/1098214005283748.

Thomas, P. A. *et al.* (eds) (2016) *Curriculum Development for Medical Education: A Six-Step Approach*. 3rd edn. Baltimore, MD: John Hopkins University Press. Available at: https://books.google.co.uk/books?id=UxF4CwAAQBAJ&printsec=frontcover.

Thomas, P., Tryfonas, T. and Sutherland, I. (2009) 'An Analysis of the Curriculum Components of Computer Forensics Undergraduate Courses in the United Kingdom', *Innovation in Teaching and Learning in Information and Computer Sciences*, 8(1), pp. 39–44.

Tomal, D. R. (2010) *Action Research for Educators*. Rowman & Littlefield Publishers.

Tomlinson, M. (2017) 'Student perceptions of themselves as "consumers" of higher education', *British Journal of Sociology of Education*, 38(4), pp. 450–467. doi: 10.1080/01425692.2015.1113856.

Tong, S. (2004) *Training the Effective Detective : A case-study examining the role of training in learning to be a detective*. phdthesis. University of Cambridge. Available at: http://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.615009 (Accessed: 4 January 2016).

Tryfonas, T. (2008) 'Developing Reusable Objects for Computer Forensics', in *9th Annual Conference of the Subject Centre for Information and Computer Sciences*. *Annual Conference of the Subject Centre for Information and Computer Sciences*, Liverpool Hope University: HE Academy (9th), p. 215. Available at: https://www.researchgate.net/profile/Thomas_Lancaster/publication/234127077_How_to_succeed_at_cheating_without_really_trying_Five_top_tips_for_successful_cheating/links/0c96053a0543beebf9000000.pdf (Accessed: 6 January 2016).

Tu, M. *et al.* (2012) 'On the Development of a Digital Forensics Curriculum', *Journal of Digital Forensics, Security and Law*, 7(3), pp. 13–32. doi: 10.15394/jdfsl.2012.1126.

Tymon, A. (2013) 'The student perspective on employability', *Studies in Higher Education*, 38(6), pp. 841–856. doi: 10.1080/03075079.2011.604408.

UCAS (2012) *End of Cycle Report 2012*. Cheltenham: Universities and Colleges Admissions Services (UCAS), p. 118. Available at: https://www.ucas.com/sites/default/files/ucas-end-of-cycle-report-2012.pdf (Accessed: 30 December 2018).

UCAS (2017a) 'EXACT Statistics Requested Definitions'.

UCAS (2017b) *UCAS Search Tool*. Available at: http://search.ucas.com/ (Accessed: 27 April 2017).

Universities and Colleges Admissions Service (UCAS) (2015) *Forensic Computing University Course Search Results*. Available at: http://search.ucas.com/search/providers?CountryCode=&RegionCode=&Lat=&Lng=&Feather=&Vac=1&AvailableIn=2016&Query=forensic+computing&ProviderQuery=&AcpId=&Location=&SubjectCode= (Accessed: 17 June 2015).

Universities and Colleges Admissions Service (UCAS) (2017) *UCAS Search Tool*. Available at: http://search.ucas.com/ (Accessed: 27 April 2017).

Universities UK (2015) *Patterns and Trends In UK Higher Education 2015*. London: Universities UK. Available at: http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2015/patterns-and-trends-2015.pdf (Accessed: 13 April 2017).

Vandermeer, Y. (no date) 'Global Cybercrime Certification'. Available at: https://rm.coe.int/3148-2-3-ecteg-17-global-cy-certif/1680727f35 (Accessed: 25 February 2019).

Vandermeer, Y. (2018) 'Cybercrime Capacity Building', in *Making the UK and Europe a safer place to live and work online*. Canterbury: Canterbury Christ Church University. Available at: https://www.canterbury.ac.uk/social-and-applied-sciences/law-criminal-justice-and-computing/docs/cyber-conference-2018/Yves-Vandermeer-Cybercrime-Capacity-Building.pdf (Accessed: 12 January 2019).

Vidalis, S., Llewellyn, E. and Angelopoulou, O. (2010) 'Educating Digital Forensic Investigators at Newport', in *The 4th International Conference on Cybercrime Forensics Education & Training*. Canterbury, UK.

Vincze, E. A. (2016) 'Challenges in digital forensics', *Police Practice and Research*, 17(2), pp. 183–194. doi: 10.1080/15614263.2015.1128163.

Visti, H. (2013) 'ForGe – Computer Forensic Test Image Generator', *Forensic Focus - Articles*, 18 October. Available at: https://articles.forensicfocus.com/2013/10/18/forge-computer-forensic-test-image-generator/ (Accessed: 12 March 2018).

Wainwright, R. (2016) 'Trends and challenges for law enforcement training and education', in *European Police Science and Research Bulletin*. Budapest, Hungary: European Union Agency for Law Enforcement Training (CEPOL (Special Conference Edition, 3), pp. 11–20. Available at: https://bulletin.cepol.europa.eu/index.php/bulletin/issue/view/23/European%20Police%20Science%20and%20Research%20Bulletin%20-%20Special%20Conference%20Edition%20n.%203 (Accessed: 15 August 2018).

Walker, J. T. and Maddan, S. (2009) *Statistics in Criminology and Criminal Justice: Analysis and Interpretation*. 3rd edn. Sudbury, MA: Jones & Bartlett Publishers. Available at: https://books.google.co.uk/books?id=VxcfI-O2iWMC&printsec=frontcover (Accessed: 8 August 2018).

Watson, W. R. and Fang, J. (2012) 'PBL as a Framework for Implementing Video Games in the Classroom':, *International Journal of Game-Based Learning*, 2(1), pp. 77–89. doi: 10.4018/ijgbl.2012010105.

Weyers, M., Strydom, H. and Huisamen, A. (2014) 'Traingulation in Social Work Research: The Theory and Examples of its Practical Application', *Social Work/Maatskaplike Werk*, 44(2). doi: 10.15270/44-2-251.

Whitten, D. (2008) 'The Chief Information Security Officer: An Analysis of the Skills Required for Success', *Journal of Computer Information Systems*, 48(3), pp. 15–19. doi: 10.1080/08874417.2008.11646017.

Whyte, W. F. (1984) *Learning from the Field: A Guide from Experience*. SAGE.

de Winter, J. C. F., Dodou, D. and Wieringa, P. A. (2009) 'Exploratory Factor Analysis With Small Sample Sizes', *Multivariate Behavioral Research*, 44(2), pp. 147–181. doi: 10.1080/00273170902794206.

Wolf, M., Shafer, A. and Gendron, M. (2006) 'Toward Understanding Digital Forensics as a Profession: Defining Curricular Needs (*** Research in Process***)', in *Proceedings of the Conference on Digital Forensics, Security and Law*, pp. 57–66. Available at: http://proceedings.adfsl.org/index.php/CDFSL/article/view/6 (Accessed: 15 April 2015).

Yasinsac, A. *et al.* (2003) 'Computer Forensics Education', *IEEE Security & Privacy*, 1(4). Available at: http://www.pmsommer.com/CSDS_Paper.pdf (Accessed: 30 March 2015).

Yiend, J. *et al.* (2016) 'Post graduate clinical placements: evaluating benefits and challenges with a mixed methods cross sectional design', *BMC Medical Education*, 16(1), p. 64. doi: 10.1186/s12909-016-0575-7.

Yusoff, Y., Ismail, R. and Hassan, Z. (2011) 'Common Phases of Computer Forensics Investigation Models', *International Journal of Computer Science & Information Technology*, 3(3), pp. 17–31. doi: 10.5121/ijcsit.2011.3302.

APPENDICES

APPENDIX A – DATA COLLECTION QUESTION EXAMPLES

This appendix includes sample questions asked throughout methods used for data collection. The questions provided may have differed depending on the semi-structure of each interview. The lists below are not an exhaustive list of the range of questions asked of each target group, however, they provide an idea on the recurring themes and measures to obtain viewpoints and experiences.

A.1 Resourcing Questionnaire

This section provides an overview of the questions which were posed to academics in a questionnaire regarding the resourcing of digital forensics programmes in higher education. The results from these questions were discussed in chapter 5.

Please state the names of the computer forensics programmes that you run and the number of students on each course (per annum).
How many labs does your department have?
How many labs contain forensic specific equipment?
How many computers in each general computing lab?
How many computers in your forensic computing specific lab(s)?
Of these, how many contain forensic software and/or hardware?
Are your laboratories solely dedicated towards the computer forensics students?
Do any of these labs have 24/7 access?
Are other departments/non-Computer Forensics programmes able to book the lab for teaching?
How often are the labs used for lectures/practicals (approx. hours per week)?
How often are the labs free for students to utilise for private study (approx. hours per week)?
Do your students have problems gaining access to the lab(s) for work purposes?
What problems do the students have in gaining access?
What solutions, if any, have you found to deal with issues relating to student access to lab(s)?
Is this due to the lab(s) being dedicated solely to Computer Forensic students?
How have you solved or attempted to solve student access problems?
Do you know the specification of your forensic specific laboratory computers?

Operating System, CPU, RAM, HDD Capacity/Speed, Number of Hard Drives, Internet Access, Separation of Forensic Network

How regularly is the hardware updated?

What year was the last time the hardware was updated?

How regularly is your software updated?

What Forensic hardware and software do you have?

Forensic Hardware Devices

Forensic Software/Licensed Products/Distributions

Do you provide any accreditation from software vendors to students? Which?

Do any of the staff who teach on the programmes have accreditations? If so, how many?

How many staff teaching this topic have commercial computer forensic experience?

A.2 Academic Interview Questions

This section highlights example questions and topics which were discussed in interviews with academics, many of which were discussed in chapter 6. The questions and topics provided below are some examples of those tackled within the interviews. Discussions took different approaches depending on the responses of the interviewees; although, identifying with similar themes in a semi-structured approach.

Can you describe your general experiences in developing digital forensic programmes?

What do you believe to be the most important design features of a digital forensics course?

Taking those experiences are there any specific ways which you believe students learn/are taught best?

What are your views on training versus education?

Do you believe the Digital Forensics curricula meets industry demands?

Do you believe there is a skills-shortage? If so, what are they and how best do you see they are approached through academia?

What are your views on accreditation?

What are your thoughts on the lack of a framework around curriculum in academia?

What is your view on experience over education?

A.3 Graduate Interview Questions

Graduates were a target group of this study and questions and topics are highlighted below to outline the essence of these interviews. Graduates were those from CCCU and results of these interviews are discussed in chapter 6. Some of the questions asked of these graduates overlap with professionals in effort to identify similar or contrasting points of view based on experience.

If you would try to remember back to when you were studying your degree, are you able to remember what your initial thoughts of the course were?

Let us take those initial thoughts, can you tell me, how and if your thoughts changed over the duration of your course?

Can you tell me what made you choose a course in Digital Forensics?

Let us take those thoughts; can you now tell me, how you judge your degree experience today?

What does your degree mean to you?

Do you feel your degree studies prepared you for your job today? Is there anything which could have prepared you more?

Did you find the subjects you learnt important? What subjects would you say you benefitted from the most in your new role?

Can you describe to me where you saw yourself in five years' time from your degree studies?

Did you find learning interesting? Is there a way in which you feel you best learn?

A.4 Professional Interview Questions

In order to discover what industry are expecting, or look for, from education and training, professional participants were required. Several interviews were conducted and themes similar to those abovementioned were approached. Below are sample questions asked of professional interviewees. Professional views were approached in chapter 7.

What are your current main responsibilities?

Do you have any input when hiring new colleagues? If so, what do you see when employing graduates?

What are your experiences with education/training?

What is usually required and/or expected of a graduate?

What do you see when employing/working with graduates?

Are there any common limitations amongst the graduates you have seen/worked with? How common are experience shortfalls?

Do you believe education can continue to fulfil the needs of the industry?

What are your thoughts on education, experience, and training?

What are your thoughts on a framework for digital forensics curriculum and any impact on graduate employability?

What are your thoughts on the current digital forensics training programmes?

Is there a skills-shortage within the current industry? If so, how do you believe it can be tackled best?

How do you believe the industry will progress and develop further?

A.5 Student Workshop Questionnaire

Students are arguably the most important part in the educational system today; this led to the identification that students needed to be a target audience of this study. Below are several questions asked of two sets of students in chapter 8, where workshops were conducted to gain these results.

Gender and Age

Have you worked in the IT-sector before?

What course are you studying?

What is your favourite way to learn?

What was your main reason for choosing digital forensics/cyber security?

What sector of employment do you want to be working in after your degree?

What job will you be aiming to obtain after your degree?

What specialism would you most like to master, or feel is most important in the current industry?

What wage would you expect to earn on graduating?

Do you believe the public are fully aware of what a digital forensics/cyber security practitioners' role is?

What do you know, or feel are the main responsibilities of a digital forensics and/or cyber security practitioner?

How important do you think the following are for a digital forensic/cyber security practitioner?

- Education
- Training
- Experience

What skills-shortages do you think current industry suffers from?

What do you think stands out for an employer from one graduate to another?

Is learning the theory of digital forensics/cyber security important?

- Why do you believe learning the theory of digital forensics/cyber security is important?
- Why do you believe learning the theory of digital forensics/cyber security not to be important?
- Why do you think maybe or unsure as to the importance of learning the theory of digital forensics/cyber security?

Are soft skills important (e.g., communication and people skills) within digital forensics/cyber security?

What were your expectations of Higher Education and the course prior to starting?

What were your views of digital forensics and/or cyber security prior to starting your course?

Were your expectations and views similar to reality and have been met by the course so far?

How could your expectations be met further?

What subjects do you think a degree in digital forensics and cyber security should include?

Fundamentals of Computing
Legal, Professional and Ethical Issues
Court Room Skills
Linux Forensics
Live Data Forensics
Linux as an Investigative Tool
Software Engineering/Development
Pen Testing Techniques and Tools
Information Security and Assurance
Networks
Operating, File and Computer Systems
Computational Mathematics
Contemporary Issues/Emerging Technologies
Project Management
Basic Forensic Procedures
Policing and Criminal Justice
Mobile Forensics
Mac Forensics
Digital Forensics Tools (Proprietary)
Digital Forensics Tools (Open Source)
Scripting/Programming
Ethical Hacking and Countermeasures
Server Infrastructure
Databases
Cryptography
Internet of Things
Employability Skills

Are there any other subjects do you think should be included in a degree in digital forensics and cyber security?

Is there anything you expect to see or be improved in your education to support graduate employability?

A.6 Public Participant Questionnaire

Public perceptions are particularly important when it comes to identifying the view of digital forensics and cyber security. Their opinions can be interesting and can show insight into what they feel is rife within the disciplines and important for their own personal gain, interests or at a more societal standpoint. Chapter 10 discussed the views of public participants in this study. Below are questions which were asked of these individuals to grasp their own understanding and perceptions of both digital forensics and cyber security.

Gender and Age

Current employment status

Highest level of education completed

What devices do you use to access the Internet?

Which of the following activities do you do online/with a digital device?

Which of these cyber-related terms are you familiar with?

Have you ever been a victim of a digital/cyber-related crime?

- What was the crime(s) you were a victim of?
- How did you respond to these incidents?
- Did you report the crime to the relevant authorities/websites?
- What was the end result?

What do you feel needs to be tackled in society in relation to digital crime and cyber security?

How often do you change your passwords?

Have you ever used one of the following as a password? (123456; password; 123456789; qwerty; 123123; google; 111111; qwertyuiop; 1q2w3e4r)

To what extent do you agree or disagree with the following statements?

- You like to use and tinker with technology?
- You are concerned about your privacy?
- You are concerned about the security of your digital devices?
- You are concerned that your personal information is not kept secure by websites
- You are not concerned about your online personal information being kept secure by public authorities
- You avoid disclosing personal information online
- You believe the risk of becoming a victim of a digital or cyber-related crime is increasing
- You believe you are able to protect yourself sufficiently against such crimes using precautions such as anti-virus software

APPENDIX B – PARTICIPANT DEMOGRAPHICS

B.1 Academic Participants

Characteristics	Total n (%)	
Gender		
Female	1	(11.1)
Male	8	(88.9)
Total	9	(100.0)
Years' Experience in Academia		
0-5 years	3	(77.8)
6-10 years	2	(22.2)
11-15 years	1	(11.1)
16-20 years	1	(11.1)
21-30 years	2	(22.2)
Total	9	(100.0)
Total Years' Experience		
0-5 years	0	(0.0)
6-10 years	1	(11.1)
11-15 years	4	(44.4)
16-20 years	1	(11.1)
21-30 years	3	(33.3)
Total	9	(100.0)

Table B.1.1 – Demographic of Academic Interviewees

B.2 Graduate Participants

Characteristics	Total n (%)	
Gender		
Female	1	(14.3)
Male	6	(85.7)
Total	7	(100.0)
Employment		
Law Enforcement	6	(85.7)
IT Industry	1	(14.3)
Total	7	(100.0)
Years' Experience		
0-1 years	3	(42.9)
2-3 years	4	(57.1)
Total	7	(100.0)

Table B.2.1 – Demographic of Graduate Participants

B.3 Student Participants

Characteristics	University A Total n	(%)	University B Total n	(%)	Total n	(%)
Gender						
Female	3	(18.80)	3	(13.04)	6	(15.38)
Male	12	(75.00)	20	(86.96)	32	(82.06)
Prefer not to say	1	(6.30)	0	(0.00)	1	(2.56)
Total	16	(100.0)	23	(100.0)	39	(100.0)
Previous work in IT-sector						
Yes	3	(18.80)	3	(13.04)	6	(15.38)
No	13	(81.30)	18	(78.26)	31	(79.49)
Free-form Response (work experience)	0	(0.00)	2	(8.70)	2	(5.13)
Total	16	(100.0)	23	(100.0)	39	(100.0)
Course						
Computer Forensics and Security	16	(100.0)	0	(0.00)	16	(41.02)
Cyber and Computer Security	0	(0.00)	11	(47.83)	11	(28.21)
Computer and Cyber Forensics	0	(0.00)	12	(52.17)	12	(30.77)
Total	16	(100.0)	23	(100.0)	39	(100.0)

Table B.3.2 – Demographic of Students as Participants

B.4 Professional Participants

Characteristics	Male n	(%)	Female n	(%)	Total n	(%)
Employment Industry						
Government	3	(11.1)	0	(0.00)	3	(10.0)
Education	2	(7.41)	0	(0.00)	2	(6.66)
Financial Services	0	(0.00)	1	(33.33)	1	(3.33)
Self employed	1	(3.70)	0	(0.00)	1	(3.33)
Law Enforcement	6	(22.22)	2	(66.67)	8	(26.66)
Police	4	(14.81)	0	(0.00)	4	(13.33)
Digital Forensics	5	(18.52)	0	(0.00)	5	(16.66)
Public Sector	2	(7.41)	0	(0.00)	2	(6.66)
DFU/DFIR	2	(7.41)	0	(0.00)	2	(6.66)
Gaming	1	(3.70)	0	(0.00)	1	(3.33)
Investigation	1	(3.70)	0	(0.00)	1	(3.33)
Total	27	(100.0)	3	(100.0)	30	(100.0)
Gender	27	(90.0)	3	(10.0)	30	(100.0)
Experience Level						
0-5 years	12	(40.0)	2	(6.66)	14	(46.66)
6-10 years	8	(26.66)	1	(3.33)	9	(30.0)
11-15 years	5	(16.66)	0	(0.00)	5	(16.66)
16-20 years	1	(3.33)	0	(0.00)	1	(3.33)
21-25 years	1	(3.33)	0	(0.00)	1	(3.33)
Total	27	(90.0)	3	(10.0)	30	(100.0)
Holds a related Higher Education Qualification						
Yes	17	(56.67)	2	(6.66)	19	(63.33)
No	10	(33.33)	1	(3.33)	11	(36.66)

Total	27	(90.00)	3	(10.0)	30	(100.0)
Input when hiring new employees						
Yes	10	(33.33)	2	(6.66)	12	(40.0)
No	10	(33.33)	1	(3.33)	11	(36.7)
Sometimes	7	(23.33)	0	(0.00)	7	(23.3)
Total	27	(90.0)	3	(10.0)	30	(100.0)

Table B.4.1 – Demographic of Professional Questionnaire Participants

B.5 Public Participants

Characteristics	Male n (%)		Female n (%)		Other n (%)		Prefer not to say n (%)		Total n (%)	
Age										
18-20	3	(2.9)	0	(0)	1	(1.0)	0	(0.0)	4	(3.9)
21-24	0	(0.0)	7	(6.9)	1	(1.0)	0	(0.0)	8	(8.8)
25-30	8	(7.8)	12	(11.8)	0	(0.0)	1	(1.0)	21	(20.6)
31-40	6	(5.9)	11	(10.8)	0	(0.0)	0	(0.0)	17	(16.7)
41-55	13	(12.7)	18	(17.6)	2	(2.0)	0	(0.0)	33	(31.4)
56-65	4	(3.9)	7	(6.9)	0	(0.0)	0	(0.0)	11	(10.8)
66+	4	(3.9)	4	(3.9)	0	(0.0)	0	(0.0)	8	(7.8)
Total	38	(37.3)	59	(57.8)	4	(3.9)	1	(1.0)	102	(100.0)
Employment										
Employed (Full-time)	26	(68.4)	41	(69.5)	4	(100.0)	1	(100.0)	72	(70.6)
Employed (Part-time)	2	(5.3)	5	(8.5)	0	(0.0)	0	(0.0)	7	(6.9)
Self-employed	5	(13.2)	2	(3.4)	0	(0.0)	0	(0.0)	7	(6.9)
Unemployed	0	(0.0)	2	(3.4)	0	(0.0)	0	(0.0)	2	(2.0)
Retired	3	(7.9)	7	(11.9)	0	(0.0)	0	(0.0)	10	(9.8)
Student (Full-time)	2	(5.3)	0	(0.0)	0	(0.0)	0	(0.0)	2	(2.0)
Student (Part-time)	0	(0.0)	1	(1.7)	0	(0.0)	0	(0.0)	1	(1.0)
Other	0	(0.0)	1	(1.7)	0	(0.0)	0	(0.0)	1	(1.0)
Total	38	(100.0)	59	(100.0)	4	(100.0)	1	(100.0)	102	(100.0)
Gender	38	(37.3)	59	(57.8)	4	(3.9)	1	(1.0)	102	(100.0)
Education										
Doctorate Degree	1	(2.6)	1	(1.7)	0	(0.0)	0	(0.0)	2	(2.0)
Master's Degree	3	(7.9)	9	(15.2)	0	(0.0)	1	(100.0)	13	(12.7)
Bachelor's Degree	12	(31.6)	16	(27.1)	2	(50.0)	0	(0.0)	30	(29.4)
Foundation Degree	1	(2.6)	0	(0.0)	0	(0.0)	0	(0.0)	1	(1.0)
A-Level or equivalent	5	(13.2)	12	(20.3)	1	(25.0)	0	(0.0)	18	(17.6)
HND/HNC/NVQ Level	5	(13.2)	5	(8.5)	0	(0.0)	0	(0.0)	10	(9.8)
GCSE level or equivalent	7	(18.4)	6	(10.2)	0	(0.0)	0	(0.0)	13	(12.7)
Some College, no degree	2	(5.3)	8	(13.6)	1	(25.0)	0	(0.0)	11	(10.8)
Trade/Technical/Vocational	2	(5.3)	2	(3.4)	0	(0.0)	0	(0.0)	4	(3.9)
Total	38	(100.0)	59	(100.0)	4	(100.0)	1	(100.0)	102	(100.0)
Gender	38	(37.3)	59	(57.8)	4	(3.9)	1	(1.0)	102	(100.0)

Table B.5.1 – Demographic of Public Questionnaire Participants

APPENDIX C – DIGITAL FORENSICS COURSE OFFERING ANALYSIS

This appendix holds all data used for analysis in section 2.3, chapter 2.

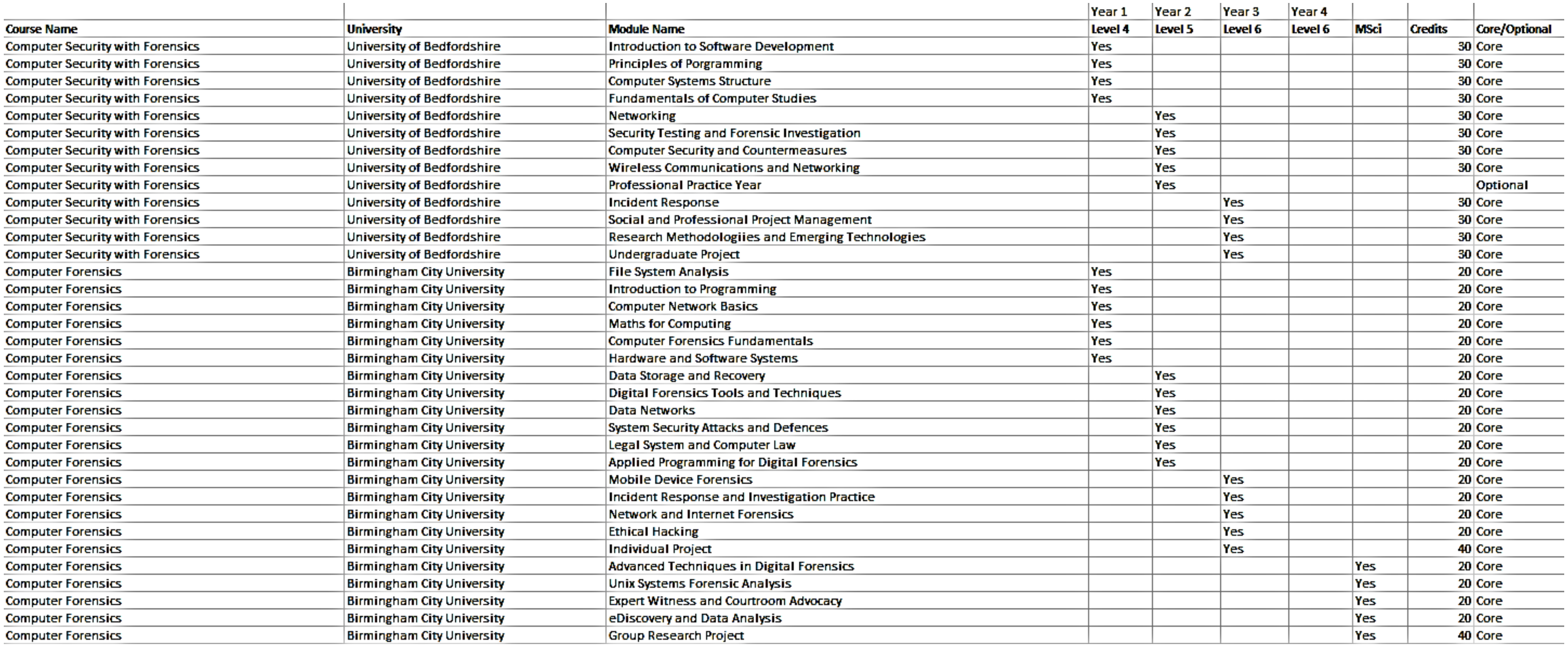
Each course offering identified has been listed, at the time of analysis. Therefore, it should be noted that these courses may have developed or amended what is on offer at the time of reading.

Section A3.1 demonstrates listings of all courses ordered by university and level of study. In some instances, module information such as credits per module and choice options are denoted.

Sections A3.2 through to A3.4 demonstrate the same courses and modules, however, present a breakdown of each university by topics analysed when conducting a keyword search noted in chapter 2.

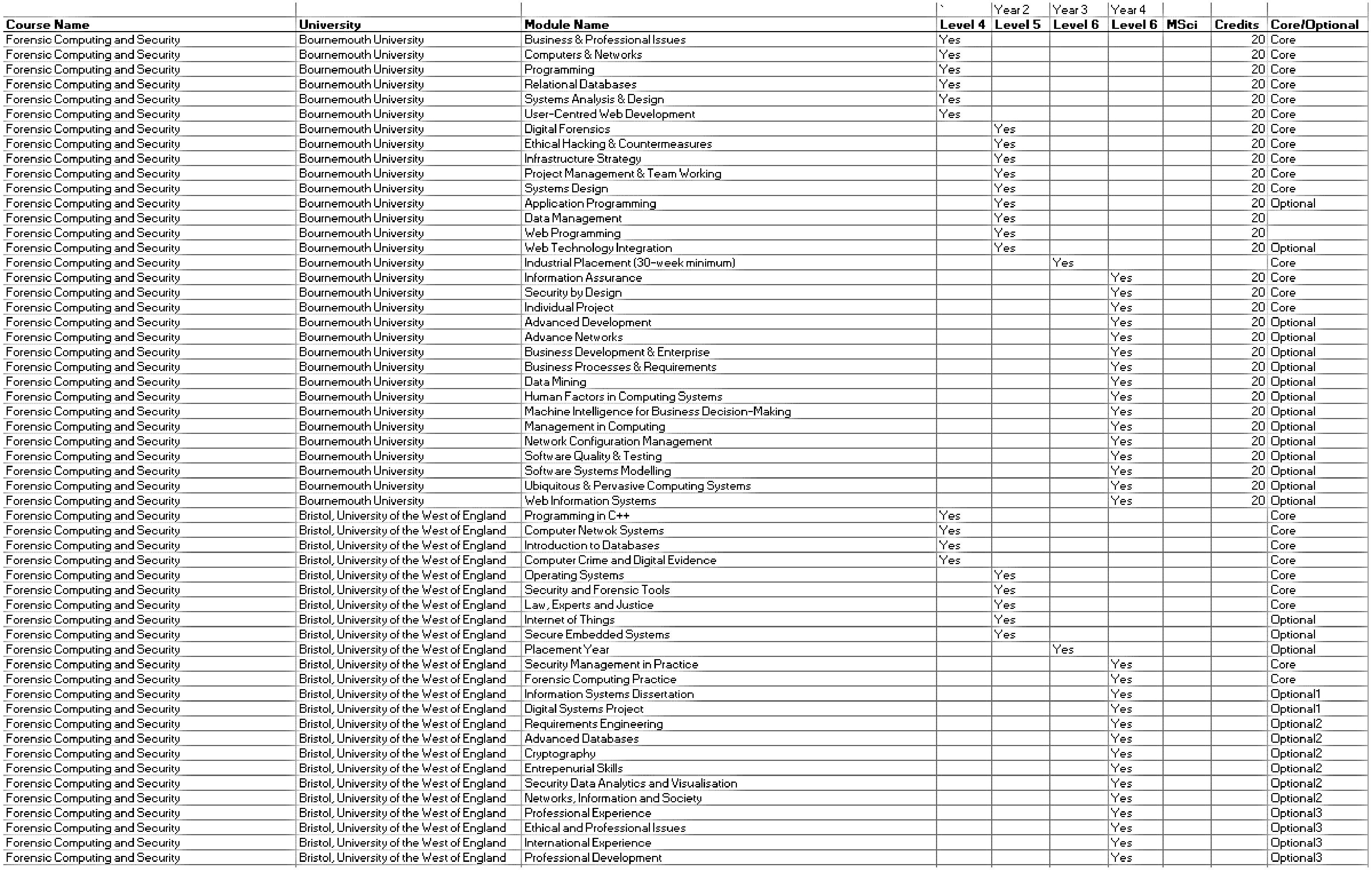
Furthermore, sections A3.5 through to A3.7 demonstrate the same data highlighted in previous sections; although, these figures are used to demonstrate solely digital forensic courses versus those including cyber security, excluding those considered in section C.7 above and considered as computer science courses with a flavour of forensics or security.

C.1 Course Offerings by University and Level of Study



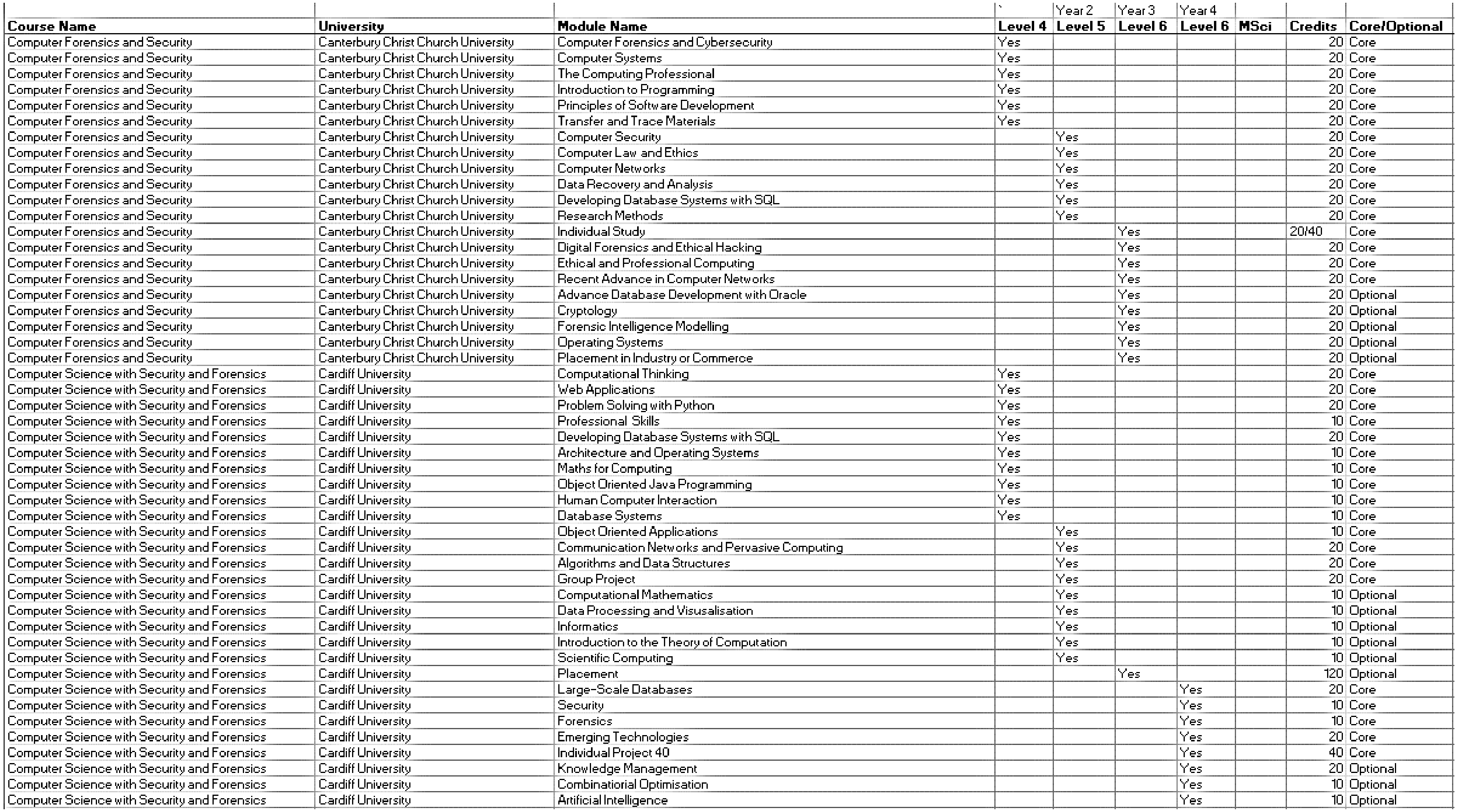
			Year 1	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Computer Security with Forensics	University of Bedfordshire	Introduction to Software Development	Yes					30	Core
Computer Security with Forensics	University of Bedfordshire	Principles of Porgramming	Yes					30	Core
Computer Security with Forensics	University of Bedfordshire	Computer Systems Structure	Yes					30	Core
Computer Security with Forensics	University of Bedfordshire	Fundamentals of Computer Studies	Yes					30	Core
Computer Security with Forensics	University of Bedfordshire	Networking		Yes				30	Core
Computer Security with Forensics	University of Bedfordshire	Security Testing and Forensic Investigation		Yes				30	Core
Computer Security with Forensics	University of Bedfordshire	Computer Security and Countermeasures		Yes				30	Core
Computer Security with Forensics	University of Bedfordshire	Wireless Communications and Networking		Yes				30	Core
Computer Security with Forensics	University of Bedfordshire	Professional Practice Year		Yes					Optional
Computer Security with Forensics	University of Bedfordshire	Incident Response			Yes			30	Core
Computer Security with Forensics	University of Bedfordshire	Social and Professional Project Management			Yes			30	Core
Computer Security with Forensics	University of Bedfordshire	Research Methodologiies and Emerging Technologies			Yes			30	Core
Computer Security with Forensics	University of Bedfordshire	Undergraduate Project			Yes			30	Core
Computer Forensics	Birmingham City University	File System Analysis	Yes					20	Core
Computer Forensics	Birmingham City University	Introduction to Programming	Yes					20	Core
Computer Forensics	Birmingham City University	Computer Network Basics	Yes					20	Core
Computer Forensics	Birmingham City University	Maths for Computing	Yes					20	Core
Computer Forensics	Birmingham City University	Computer Forensics Fundamentals	Yes					20	Core
Computer Forensics	Birmingham City University	Hardware and Software Systems	Yes					20	Core
Computer Forensics	Birmingham City University	Data Storage and Recovery		Yes				20	Core
Computer Forensics	Birmingham City University	Digital Forensics Tools and Techniques		Yes				20	Core
Computer Forensics	Birmingham City University	Data Networks		Yes				20	Core
Computer Forensics	Birmingham City University	System Security Attacks and Defences		Yes				20	Core
Computer Forensics	Birmingham City University	Legal System and Computer Law		Yes				20	Core
Computer Forensics	Birmingham City University	Applied Programming for Digital Forensics		Yes				20	Core
Computer Forensics	Birmingham City University	Mobile Device Forensics			Yes			20	Core
Computer Forensics	Birmingham City University	Incident Response and Investigation Practice			Yes			20	Core
Computer Forensics	Birmingham City University	Network and Internet Forensics			Yes			20	Core
Computer Forensics	Birmingham City University	Ethical Hacking			Yes			20	Core
Computer Forensics	Birmingham City University	Individual Project			Yes			40	Core
Computer Forensics	Birmingham City University	Advanced Techniques in Digital Forensics					Yes	20	Core
Computer Forensics	Birmingham City University	Unix Systems Forensic Analysis					Yes	20	Core
Computer Forensics	Birmingham City University	Expert Witness and Courtroom Advocacy					Yes	20	Core
Computer Forensics	Birmingham City University	eDiscovery and Data Analysis					Yes	20	Core
Computer Forensics	Birmingham City University	Group Research Project					Yes	40	Core

Figure C.1.1 Course offerings by university and level of study



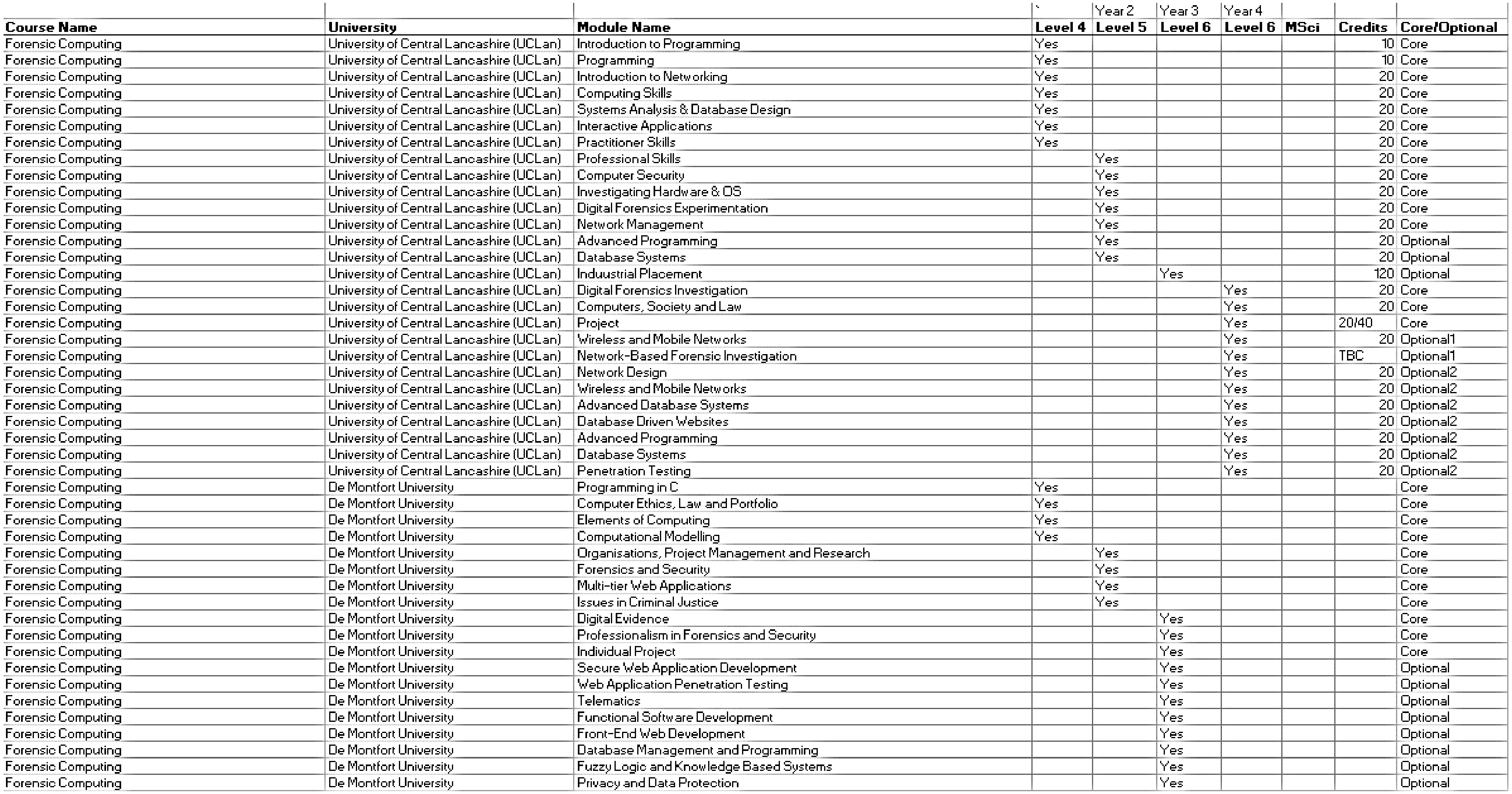
			`	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Forensic Computing and Security	Bournemouth University	Business & Professional Issues	Yes					20	Core
Forensic Computing and Security	Bournemouth University	Computers & Networks	Yes					20	Core
Forensic Computing and Security	Bournemouth University	Programming	Yes					20	Core
Forensic Computing and Security	Bournemouth University	Relational Databases	Yes					20	Core
Forensic Computing and Security	Bournemouth University	Systems Analysis & Design	Yes					20	Core
Forensic Computing and Security	Bournemouth University	User-Centred Web Development	Yes					20	Core
Forensic Computing and Security	Bournemouth University	Digital Forensics		Yes				20	Core
Forensic Computing and Security	Bournemouth University	Ethical Hacking & Countermeasures		Yes				20	Core
Forensic Computing and Security	Bournemouth University	Infrastructure Strategy		Yes				20	Core
Forensic Computing and Security	Bournemouth University	Project Management & Team Working		Yes				20	Core
Forensic Computing and Security	Bournemouth University	Systems Design		Yes				20	Core
Forensic Computing and Security	Bournemouth University	Application Programming		Yes				20	Optional
Forensic Computing and Security	Bournemouth University	Data Management		Yes				20	
Forensic Computing and Security	Bournemouth University	Web Programming		Yes				20	
Forensic Computing and Security	Bournemouth University	Web Technology Integration		Yes				20	Optional
Forensic Computing and Security	Bournemouth University	Industrial Placement (30-week minimum)			Yes				Core
Forensic Computing and Security	Bournemouth University	Information Assurance				Yes		20	Core
Forensic Computing and Security	Bournemouth University	Security by Design				Yes		20	Core
Forensic Computing and Security	Bournemouth University	Individual Project				Yes		20	Core
Forensic Computing and Security	Bournemouth University	Advanced Development				Yes		20	Optional
Forensic Computing and Security	Bournemouth University	Advance Networks				Yes		20	Optional
Forensic Computing and Security	Bournemouth University	Business Development & Enterprise				Yes		20	Optional
Forensic Computing and Security	Bournemouth University	Business Processes & Requirements				Yes		20	Optional
Forensic Computing and Security	Bournemouth University	Data Mining				Yes		20	Optional
Forensic Computing and Security	Bournemouth University	Human Factors in Computing Systems				Yes		20	Optional
Forensic Computing and Security	Bournemouth University	Machine Intelligence for Business Decision-Making				Yes		20	Optional
Forensic Computing and Security	Bournemouth University	Management in Computing				Yes		20	Optional
Forensic Computing and Security	Bournemouth University	Network Configuration Management				Yes		20	Optional
Forensic Computing and Security	Bournemouth University	Software Quality & Testing				Yes		20	Optional
Forensic Computing and Security	Bournemouth University	Software Systems Modelling				Yes		20	Optional
Forensic Computing and Security	Bournemouth University	Ubiquitous & Pervasive Computing Systems				Yes		20	Optional
Forensic Computing and Security	Bournemouth University	Web Information Systems				Yes		20	Optional
Forensic Computing and Security	Bristol, University of the West of England	Programming in C++	Yes						Core
Forensic Computing and Security	Bristol, University of the West of England	Computer Netwok Systems	Yes						Core
Forensic Computing and Security	Bristol, University of the West of England	Introduction to Databases	Yes						Core
Forensic Computing and Security	Bristol, University of the West of England	Computer Crime and Digital Evidence	Yes						Core
Forensic Computing and Security	Bristol, University of the West of England	Operating Systems		Yes					Core
Forensic Computing and Security	Bristol, University of the West of England	Security and Forensic Tools		Yes					Core
Forensic Computing and Security	Bristol, University of the West of England	Law, Experts and Justice		Yes					Core
Forensic Computing and Security	Bristol, University of the West of England	Internet of Things		Yes					Optional
Forensic Computing and Security	Bristol, University of the West of England	Secure Embedded Systems		Yes					Optional
Forensic Computing and Security	Bristol, University of the West of England	Placement Year			Yes				Optional
Forensic Computing and Security	Bristol, University of the West of England	Security Management in Practice				Yes			Core
Forensic Computing and Security	Bristol, University of the West of England	Forensic Computing Practice				Yes			Core
Forensic Computing and Security	Bristol, University of the West of England	Information Systems Dissertation				Yes			Optional1
Forensic Computing and Security	Bristol, University of the West of England	Digital Systems Project				Yes			Optional1
Forensic Computing and Security	Bristol, University of the West of England	Requirements Engineering				Yes			Optional2
Forensic Computing and Security	Bristol, University of the West of England	Advanced Databases				Yes			Optional2
Forensic Computing and Security	Bristol, University of the West of England	Cryptography				Yes			Optional2
Forensic Computing and Security	Bristol, University of the West of England	Entrepenurial Skills				Yes			Optional2
Forensic Computing and Security	Bristol, University of the West of England	Security Data Analytics and Visualisation				Yes			Optional2
Forensic Computing and Security	Bristol, University of the West of England	Networks, Information and Society				Yes			Optional2
Forensic Computing and Security	Bristol, University of the West of England	Professional Experience				Yes			Optional3
Forensic Computing and Security	Bristol, University of the West of England	Ethical and Professional Issues				Yes			Optional3
Forensic Computing and Security	Bristol, University of the West of England	International Experience				Yes			Optional3
Forensic Computing and Security	Bristol, University of the West of England	Professional Development				Yes			Optional3

Figure C.1.2 Course offerings by university and level of study



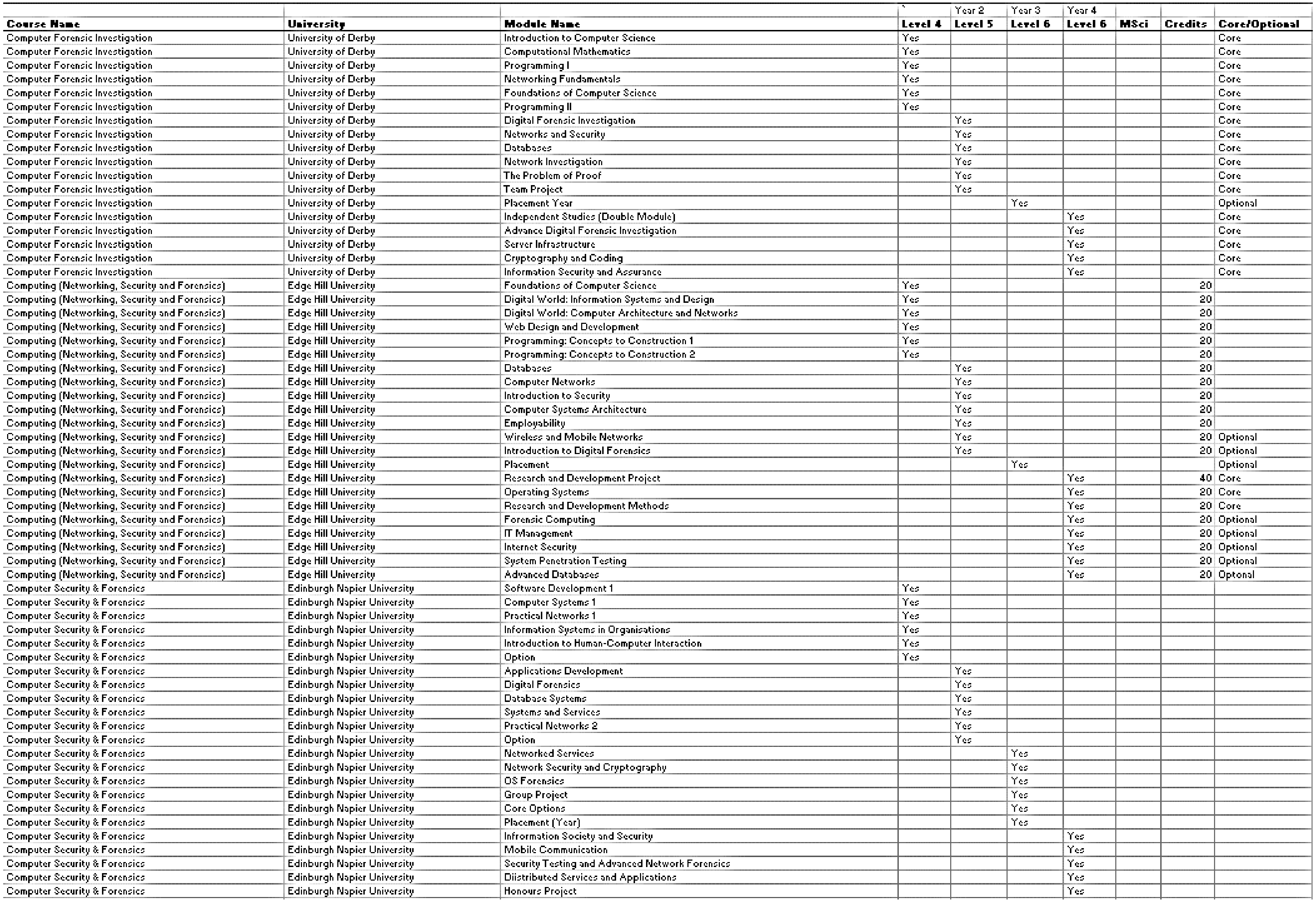
			`	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Computer Forensics and Security	Canterbury Christ Church University	Computer Forensics and Cybersecurity	Yes					20	Core
Computer Forensics and Security	Canterbury Christ Church University	Computer Systems	Yes					20	Core
Computer Forensics and Security	Canterbury Christ Church University	The Computing Professional	Yes					20	Core
Computer Forensics and Security	Canterbury Christ Church University	Introduction to Programming	Yes					20	Core
Computer Forensics and Security	Canterbury Christ Church University	Principles of Software Development	Yes					20	Core
Computer Forensics and Security	Canterbury Christ Church University	Transfer and Trace Materials	Yes					20	Core
Computer Forensics and Security	Canterbury Christ Church University	Computer Security		Yes				20	Core
Computer Forensics and Security	Canterbury Christ Church University	Computer Law and Ethics		Yes				20	Core
Computer Forensics and Security	Canterbury Christ Church University	Computer Networks		Yes				20	Core
Computer Forensics and Security	Canterbury Christ Church University	Data Recovery and Analysis		Yes				20	Core
Computer Forensics and Security	Canterbury Christ Church University	Developing Database Systems with SQL		Yes				20	Core
Computer Forensics and Security	Canterbury Christ Church University	Research Methods		Yes				20	Core
Computer Forensics and Security	Canterbury Christ Church University	Individual Study			Yes			20/40	Core
Computer Forensics and Security	Canterbury Christ Church University	Digital Forensics and Ethical Hacking			Yes			20	Core
Computer Forensics and Security	Canterbury Christ Church University	Ethical and Professional Computing			Yes			20	Core
Computer Forensics and Security	Canterbury Christ Church University	Recent Advance in Computer Networks			Yes			20	Core
Computer Forensics and Security	Canterbury Christ Church University	Advance Database Development with Oracle			Yes			20	Optional
Computer Forensics and Security	Canterbury Christ Church University	Cryptology			Yes			20	Optional
Computer Forensics and Security	Canterbury Christ Church University	Forensic Intelligence Modelling			Yes			20	Optional
Computer Forensics and Security	Canterbury Christ Church University	Operating Systems			Yes			20	Optional
Computer Forensics and Security	Canterbury Christ Church University	Placement in Industry or Commerce			Yes			20	Optional
Computer Science with Security and Forensics	Cardiff University	Computational Thinking	Yes					20	Core
Computer Science with Security and Forensics	Cardiff University	Web Applications	Yes					20	Core
Computer Science with Security and Forensics	Cardiff University	Problem Solving with Python	Yes					20	Core
Computer Science with Security and Forensics	Cardiff University	Professional Skills	Yes					10	Core
Computer Science with Security and Forensics	Cardiff University	Developing Database Systems with SQL	Yes					20	Core
Computer Science with Security and Forensics	Cardiff University	Architecture and Operating Systems	Yes					10	Core
Computer Science with Security and Forensics	Cardiff University	Maths for Computing	Yes					10	Core
Computer Science with Security and Forensics	Cardiff University	Object Oriented Java Programming	Yes					10	Core
Computer Science with Security and Forensics	Cardiff University	Human Computer Interaction	Yes					10	Core
Computer Science with Security and Forensics	Cardiff University	Database Systems	Yes					10	Core
Computer Science with Security and Forensics	Cardiff University	Object Oriented Applications		Yes				10	Core
Computer Science with Security and Forensics	Cardiff University	Communication Networks and Pervasive Computing		Yes				20	Core
Computer Science with Security and Forensics	Cardiff University	Algorithms and Data Structures		Yes				20	Core
Computer Science with Security and Forensics	Cardiff University	Group Project		Yes				20	Core
Computer Science with Security and Forensics	Cardiff University	Computational Mathematics		Yes				10	Optional
Computer Science with Security and Forensics	Cardiff University	Data Processing and Visusalisation		Yes				10	Optional
Computer Science with Security and Forensics	Cardiff University	Informatics		Yes				10	Optional
Computer Science with Security and Forensics	Cardiff University	Introduction to the Theory of Computation		Yes				10	Optional
Computer Science with Security and Forensics	Cardiff University	Scientific Computing		Yes				10	Optional
Computer Science with Security and Forensics	Cardiff University	Placement			Yes			120	Optional
Computer Science with Security and Forensics	Cardiff University	Large-Scale Databases				Yes		20	Core
Computer Science with Security and Forensics	Cardiff University	Security				Yes		10	Core
Computer Science with Security and Forensics	Cardiff University	Forensics				Yes		10	Core
Computer Science with Security and Forensics	Cardiff University	Emerging Technologies				Yes		20	Core
Computer Science with Security and Forensics	Cardiff University	Individual Project 40				Yes		40	Core
Computer Science with Security and Forensics	Cardiff University	Knowledge Management				Yes		20	Optional
Computer Science with Security and Forensics	Cardiff University	Combinatiorial Optimisation				Yes		10	Optional
Computer Science with Security and Forensics	Cardiff University	Artificial Intelligence				Yes		10	Optional

Figure C.1.3 Course offerings by university and level of study



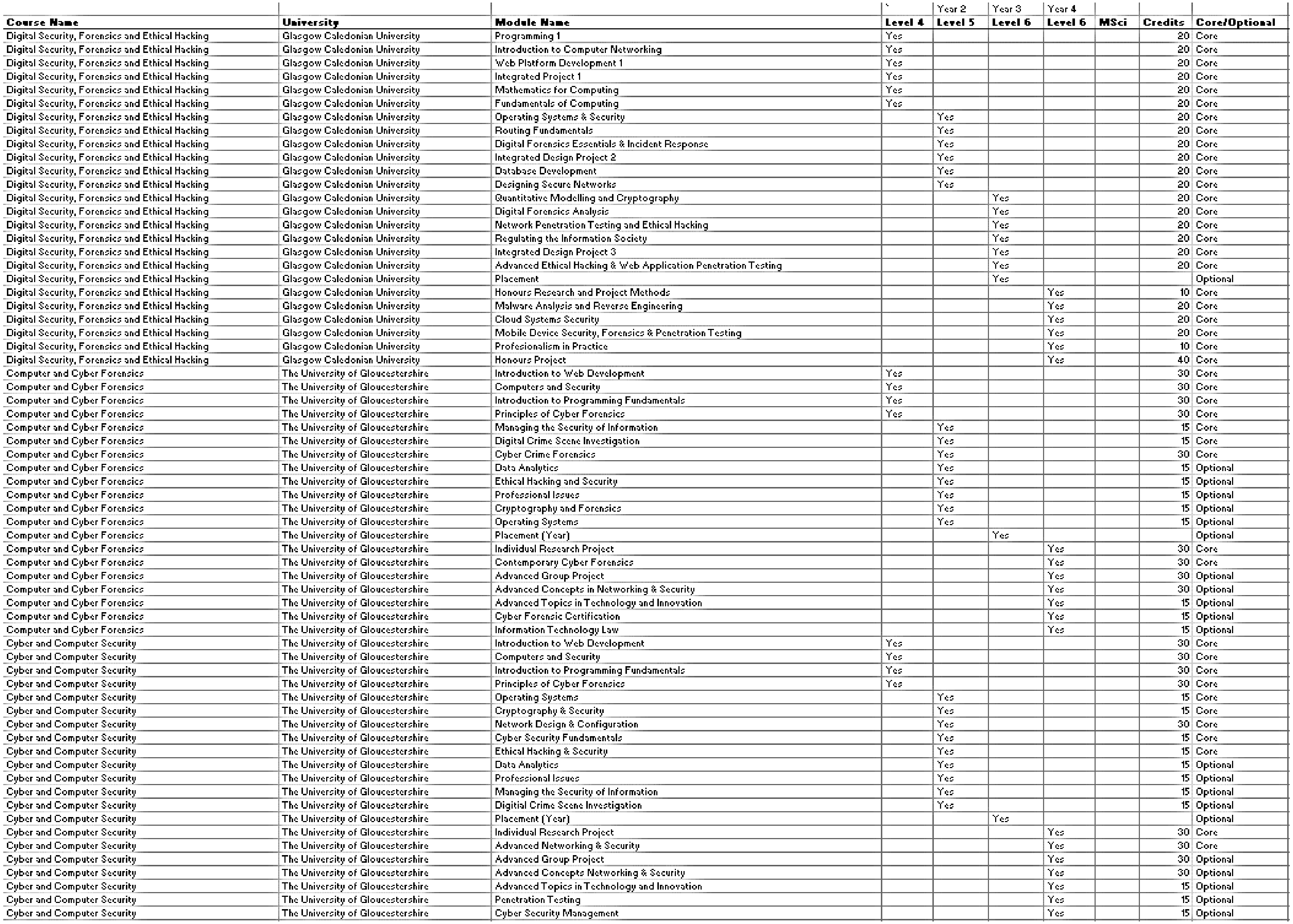
			`	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Forensic Computing	University of Central Lancashire (UCLan)	Introduction to Programming	Yes					10	Core
Forensic Computing	University of Central Lancashire (UCLan)	Programming	Yes					10	Core
Forensic Computing	University of Central Lancashire (UCLan)	Introduction to Networking	Yes					20	Core
Forensic Computing	University of Central Lancashire (UCLan)	Computing Skills	Yes					20	Core
Forensic Computing	University of Central Lancashire (UCLan)	Systems Analysis & Database Design	Yes					20	Core
Forensic Computing	University of Central Lancashire (UCLan)	Interactive Applications	Yes					20	Core
Forensic Computing	University of Central Lancashire (UCLan)	Practitioner Skills	Yes					20	Core
Forensic Computing	University of Central Lancashire (UCLan)	Professional Skills		Yes				20	Core
Forensic Computing	University of Central Lancashire (UCLan)	Computer Security		Yes				20	Core
Forensic Computing	University of Central Lancashire (UCLan)	Investigating Hardware & OS		Yes				20	Core
Forensic Computing	University of Central Lancashire (UCLan)	Digital Forensics Experimentation		Yes				20	Core
Forensic Computing	University of Central Lancashire (UCLan)	Network Management		Yes				20	Core
Forensic Computing	University of Central Lancashire (UCLan)	Advanced Programming		Yes				20	Optional
Forensic Computing	University of Central Lancashire (UCLan)	Database Systems		Yes				20	Optional
Forensic Computing	University of Central Lancashire (UCLan)	Induustrial Placement			Yes			120	Optional
Forensic Computing	University of Central Lancashire (UCLan)	Digital Forensics Investigation				Yes		20	Core
Forensic Computing	University of Central Lancashire (UCLan)	Computers, Society and Law				Yes		20	Core
Forensic Computing	University of Central Lancashire (UCLan)	Project				Yes		20/40	Core
Forensic Computing	University of Central Lancashire (UCLan)	Wireless and Mobile Networks				Yes		20	Optional1
Forensic Computing	University of Central Lancashire (UCLan)	Network-Based Forensic Investigation				Yes		TBC	Optional1
Forensic Computing	University of Central Lancashire (UCLan)	Network Design				Yes		20	Optional2
Forensic Computing	University of Central Lancashire (UCLan)	Wireless and Mobile Networks				Yes		20	Optional2
Forensic Computing	University of Central Lancashire (UCLan)	Advanced Database Systems				Yes		20	Optional2
Forensic Computing	University of Central Lancashire (UCLan)	Database Driven Websites				Yes		20	Optional2
Forensic Computing	University of Central Lancashire (UCLan)	Advanced Programming				Yes		20	Optional2
Forensic Computing	University of Central Lancashire (UCLan)	Database Systems				Yes		20	Optional2
Forensic Computing	University of Central Lancashire (UCLan)	Penetration Testing				Yes		20	Optional2
Forensic Computing	De Montfort University	Programming in C	Yes						Core
Forensic Computing	De Montfort University	Computer Ethics, Law and Portfolio	Yes						Core
Forensic Computing	De Montfort University	Elements of Computing	Yes						Core
Forensic Computing	De Montfort University	Computational Modelling	Yes						Core
Forensic Computing	De Montfort University	Organisations, Project Management and Research		Yes					Core
Forensic Computing	De Montfort University	Forensics and Security		Yes					Core
Forensic Computing	De Montfort University	Multi-tier Web Applications		Yes					Core
Forensic Computing	De Montfort University	Issues in Criminal Justice		Yes					Core
Forensic Computing	De Montfort University	Digital Evidence			Yes				Core
Forensic Computing	De Montfort University	Professionalism in Forensics and Security			Yes				Core
Forensic Computing	De Montfort University	Individual Project			Yes				Core
Forensic Computing	De Montfort University	Secure Web Application Development			Yes				Optional
Forensic Computing	De Montfort University	Web Application Penetration Testing			Yes				Optional
Forensic Computing	De Montfort University	Telematics			Yes				Optional
Forensic Computing	De Montfort University	Functional Software Development			Yes				Optional
Forensic Computing	De Montfort University	Front-End Web Development			Yes				Optional
Forensic Computing	De Montfort University	Database Management and Programming			Yes				Optional
Forensic Computing	De Montfort University	Fuzzy Logic and Knowledge Based Systems			Yes				Optional
Forensic Computing	De Montfort University	Privacy and Data Protection			Yes				Optional

Figure C.1.4 Course offerings by university and level of study



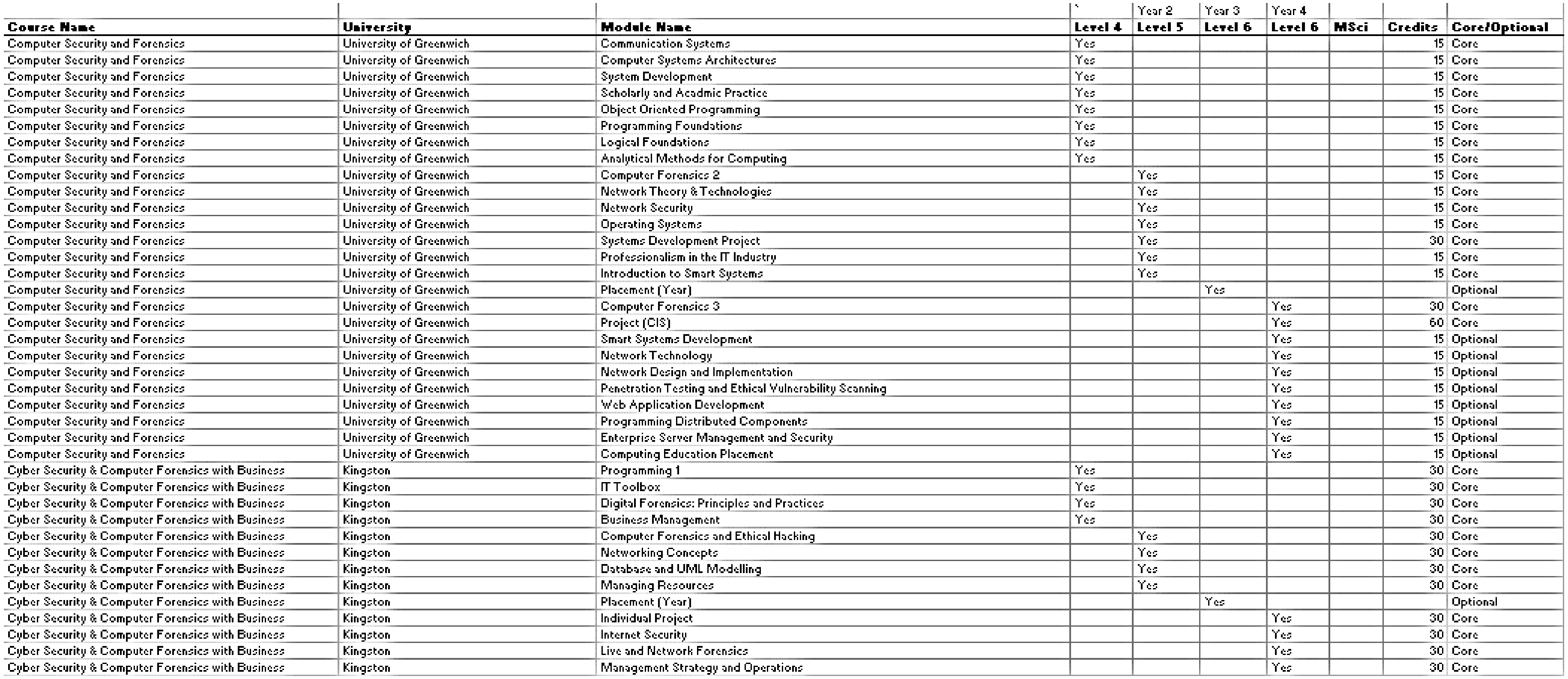
			`	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Computer Forensic Investigation	University of Derby	Introduction to Computer Science	Yes						Core
Computer Forensic Investigation	University of Derby	Computational Mathematics	Yes						Core
Computer Forensic Investigation	University of Derby	Programming I	Yes						Core
Computer Forensic Investigation	University of Derby	Networking Fundamentals	Yes						Core
Computer Forensic Investigation	University of Derby	Foundations of Computer Science	Yes						Core
Computer Forensic Investigation	University of Derby	Programming II	Yes						Core
Computer Forensic Investigation	University of Derby	Digital Forensic Investigation		Yes					Core
Computer Forensic Investigation	University of Derby	Networks and Security		Yes					Core
Computer Forensic Investigation	University of Derby	Databases		Yes					Core
Computer Forensic Investigation	University of Derby	Network Investigation		Yes					Core
Computer Forensic Investigation	University of Derby	The Problem of Proof		Yes					Core
Computer Forensic Investigation	University of Derby	Team Project		Yes					Core
Computer Forensic Investigation	University of Derby	Placement Year			Yes				Optional
Computer Forensic Investigation	University of Derby	Independent Studies (Double Module)				Yes			Core
Computer Forensic Investigation	University of Derby	Advance Digital Forensic Investigation				Yes			Core
Computer Forensic Investigation	University of Derby	Server Infrastructure				Yes			Core
Computer Forensic Investigation	University of Derby	Cryptography and Coding				Yes			Core
Computer Forensic Investigation	University of Derby	Information Security and Assurance				Yes			Core
Computing (Networking, Security and Forensics)	Edge Hill University	Foundations of Computer Science	Yes					20	
Computing (Networking, Security and Forensics)	Edge Hill University	Digital World: Information Systems and Design	Yes					20	
Computing (Networking, Security and Forensics)	Edge Hill University	Digital World: Computer Architecture and Networks	Yes					20	
Computing (Networking, Security and Forensics)	Edge Hill University	Web Design and Development	Yes					20	
Computing (Networking, Security and Forensics)	Edge Hill University	Programming: Concepts to Construction 1	Yes					20	
Computing (Networking, Security and Forensics)	Edge Hill University	Programming: Concepts to Construction 2	Yes					20	
Computing (Networking, Security and Forensics)	Edge Hill University	Databases		Yes				20	
Computing (Networking, Security and Forensics)	Edge Hill University	Computer Networks		Yes				20	
Computing (Networking, Security and Forensics)	Edge Hill University	Introduction to Security		Yes				20	
Computing (Networking, Security and Forensics)	Edge Hill University	Computer Systems Architecture		Yes				20	
Computing (Networking, Security and Forensics)	Edge Hill University	Employability		Yes				20	
Computing (Networking, Security and Forensics)	Edge Hill University	Wireless and Mobile Networks		Yes				20	Optional
Computing (Networking, Security and Forensics)	Edge Hill University	Introduction to Digital Forensics		Yes				20	Optional
Computing (Networking, Security and Forensics)	Edge Hill University	Placement			Yes				Optional
Computing (Networking, Security and Forensics)	Edge Hill University	Research and Development Project				Yes		40	Core
Computing (Networking, Security and Forensics)	Edge Hill University	Operating Systems				Yes		20	Core
Computing (Networking, Security and Forensics)	Edge Hill University	Research and Development Methods				Yes		20	Core
Computing (Networking, Security and Forensics)	Edge Hill University	Forensic Computing				Yes		20	Optional
Computing (Networking, Security and Forensics)	Edge Hill University	IT Management				Yes		20	Optional
Computing (Networking, Security and Forensics)	Edge Hill University	Internet Security				Yes		20	Optional
Computing (Networking, Security and Forensics)	Edge Hill University	System Penetration Testing				Yes		20	Optional
Computing (Networking, Security and Forensics)	Edge Hill University	Advanced Databases				Yes		20	Optonal
Computer Security & Forensics	Edinburgh Napier University	Software Development 1	Yes						
Computer Security & Forensics	Edinburgh Napier University	Computer Systems 1	Yes						
Computer Security & Forensics	Edinburgh Napier University	Practical Networks 1	Yes						
Computer Security & Forensics	Edinburgh Napier University	Information Systems in Organisations	Yes						
Computer Security & Forensics	Edinburgh Napier University	Introduction to Human-Computer Interaction	Yes						
Computer Security & Forensics	Edinburgh Napier University	Option	Yes						
Computer Security & Forensics	Edinburgh Napier University	Applications Development		Yes					
Computer Security & Forensics	Edinburgh Napier University	Digital Forensics		Yes					
Computer Security & Forensics	Edinburgh Napier University	Database Systems		Yes					
Computer Security & Forensics	Edinburgh Napier University	Systems and Services		Yes					
Computer Security & Forensics	Edinburgh Napier University	Practical Networks 2		Yes					
Computer Security & Forensics	Edinburgh Napier University	Option		Yes					
Computer Security & Forensics	Edinburgh Napier University	Networked Services			Yes				
Computer Security & Forensics	Edinburgh Napier University	Network Security and Cryptography			Yes				
Computer Security & Forensics	Edinburgh Napier University	OS Forensics			Yes				
Computer Security & Forensics	Edinburgh Napier University	Group Project			Yes				
Computer Security & Forensics	Edinburgh Napier University	Core Options			Yes				
Computer Security & Forensics	Edinburgh Napier University	Placement (Year)			Yes				
Computer Security & Forensics	Edinburgh Napier University	Infrormation Society and Security				Yes			
Computer Security & Forensics	Edinburgh Napier University	Mobile Communication				Yes			
Computer Security & Forensics	Edinburgh Napier University	Security Testing and Advanced Network Forensics				Yes			
Computer Security & Forensics	Edinburgh Napier University	Diistributed Services and Applications				Yes			
Computer Security & Forensics	Edinburgh Napier University	Honours Project				Yes			

Figure C.1.5 Course offerings by university and level of study



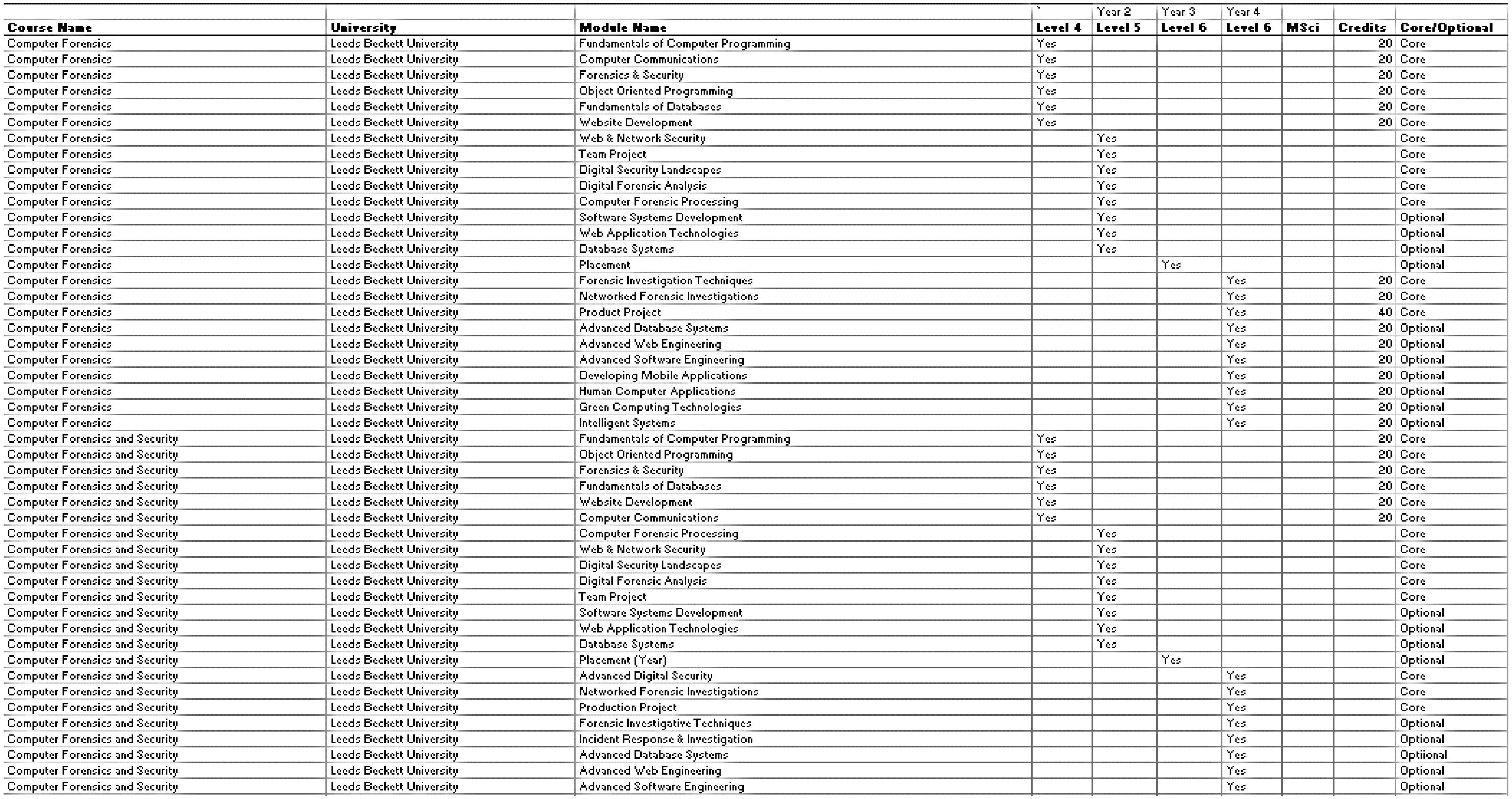
			`	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Programming 1	Yes					20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Introduction to Computer Networking	Yes					20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Web Platform Development 1	Yes					20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Integrated Project 1	Yes					20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Mathematics for Computing	Yes					20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Fundamentals of Computing	Yes					20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Operating Systems & Security		Yes				20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Routing Fundamentals		Yes				20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Digital Forensics Essentials & Incident Response		Yes				20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Integrated Design Project 2		Yes				20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Database Development		Yes				20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Designing Secure Networks		Yes				20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Quantitative Modelling and Cryptography			Yes			20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Digital Forensics Analysis			Yes			20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Network Penetration Testing and Ethical Hacking			Yes			20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Regulating the Information Society			Yes			20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Integrated Design Project 3			Yes			20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Advanced Ethical Hacking & Web Application Penetration Testing			Yes			20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Placement			Yes				Optional
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Honours Research and Project Methods				Yes		10	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Malware Analysis and Reverse Engineering				Yes		20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Cloud Systems Security				Yes		20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Mobile Device Security, Forensics & Penetration Testing				Yes		20	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Profesionalism in Practice				Yes		10	Core
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	Honours Project				Yes		40	Core
Computer and Cyber Forensics	The University of Gloucestershire	Introduction to Web Development	Yes					30	Core
Computer and Cyber Forensics	The University of Gloucestershire	Computers and Security	Yes					30	Core
Computer and Cyber Forensics	The University of Gloucestershire	Introduction to Programming Fundamentals	Yes					30	Core
Computer and Cyber Forensics	The University of Gloucestershire	Principles of Cyber Forensics	Yes					30	Core
Computer and Cyber Forensics	The University of Gloucestershire	Managing the Security of Information		Yes				15	Core
Computer and Cyber Forensics	The University of Gloucestershire	Digital Crime Scene Investigation		Yes				15	Core
Computer and Cyber Forensics	The University of Gloucestershire	Cyber Crime Forensics		Yes				30	Core
Computer and Cyber Forensics	The University of Gloucestershire	Data Analytics		Yes				15	Optional
Computer and Cyber Forensics	The University of Gloucestershire	Ethical Hacking and Security		Yes				15	Optional
Computer and Cyber Forensics	The University of Gloucestershire	Professional Issues		Yes				15	Optional
Computer and Cyber Forensics	The University of Gloucestershire	Cryptography and Forensics		Yes				15	Optional
Computer and Cyber Forensics	The University of Gloucestershire	Operating Systems		Yes				15	Optional
Computer and Cyber Forensics	The University of Gloucestershire	Placement (Year)			Yes				Optional
Computer and Cyber Forensics	The University of Gloucestershire	Individual Research Project				Yes		30	Core
Computer and Cyber Forensics	The University of Gloucestershire	Contemporary Cyber Forensics				Yes		30	Core
Computer and Cyber Forensics	The University of Gloucestershire	Advanced Group Project				Yes		30	Optional
Computer and Cyber Forensics	The University of Gloucestershire	Advanced Concepts in Networking & Security				Yes		30	Optional
Computer and Cyber Forensics	The University of Gloucestershire	Advanced Topics in Technology and Innovation				Yes		15	Optional
Computer and Cyber Forensics	The University of Gloucestershire	Cyber Forensic Certification				Yes		15	Optional
Computer and Cyber Forensics	The University of Gloucestershire	Information Technology Law				Yes		15	Optional
Cyber and Computer Security	The University of Gloucestershire	Introduction to Web Development	Yes					30	Core
Cyber and Computer Security	The University of Gloucestershire	Computers and Security	Yes					30	Core
Cyber and Computer Security	The University of Gloucestershire	Introduction to Programming Fundamentals	Yes					30	Core
Cyber and Computer Security	The University of Gloucestershire	Principles of Cyber Forensics	Yes					30	Core
Cyber and Computer Security	The University of Gloucestershire	Operating Systems		Yes				15	Core
Cyber and Computer Security	The University of Gloucestershire	Cryptography & Security		Yes				15	Core
Cyber and Computer Security	The University of Gloucestershire	Network Design & Configuration		Yes				30	Core
Cyber and Computer Security	The University of Gloucestershire	Cyber Security Fundamentals		Yes				15	Core
Cyber and Computer Security	The University of Gloucestershire	Ethical Hacking & Security		Yes				15	Core
Cyber and Computer Security	The University of Gloucestershire	Data Analytics		Yes				15	Optional
Cyber and Computer Security	The University of Gloucestershire	Professional Issues		Yes				15	Optional
Cyber and Computer Security	The University of Gloucestershire	Managing the Security of Information		Yes				15	Optional
Cyber and Computer Security	The University of Gloucestershire	Digitial Crime Scene Investigation		Yes				15	Optional
Cyber and Computer Security	The University of Gloucestershire	Placement (Year)			Yes				Optional
Cyber and Computer Security	The University of Gloucestershire	Individual Research Project				Yes		30	Core
Cyber and Computer Security	The University of Gloucestershire	Advanced Networking & Security				Yes		30	Core
Cyber and Computer Security	The University of Gloucestershire	Advanced Group Project				Yes		30	Optional
Cyber and Computer Security	The University of Gloucestershire	Advanced Concepts Networking & Security				Yes		30	Optional
Cyber and Computer Security	The University of Gloucestershire	Advanced Topics in Technology and Innovation				Yes		15	Optional
Cyber and Computer Security	The University of Gloucestershire	Penetration Testing				Yes		15	Optional
Cyber and Computer Security	The University of Gloucestershire	Cyber Security Management				Yes		15	Optional

Figure C.1.6 Course offerings by university and level of study



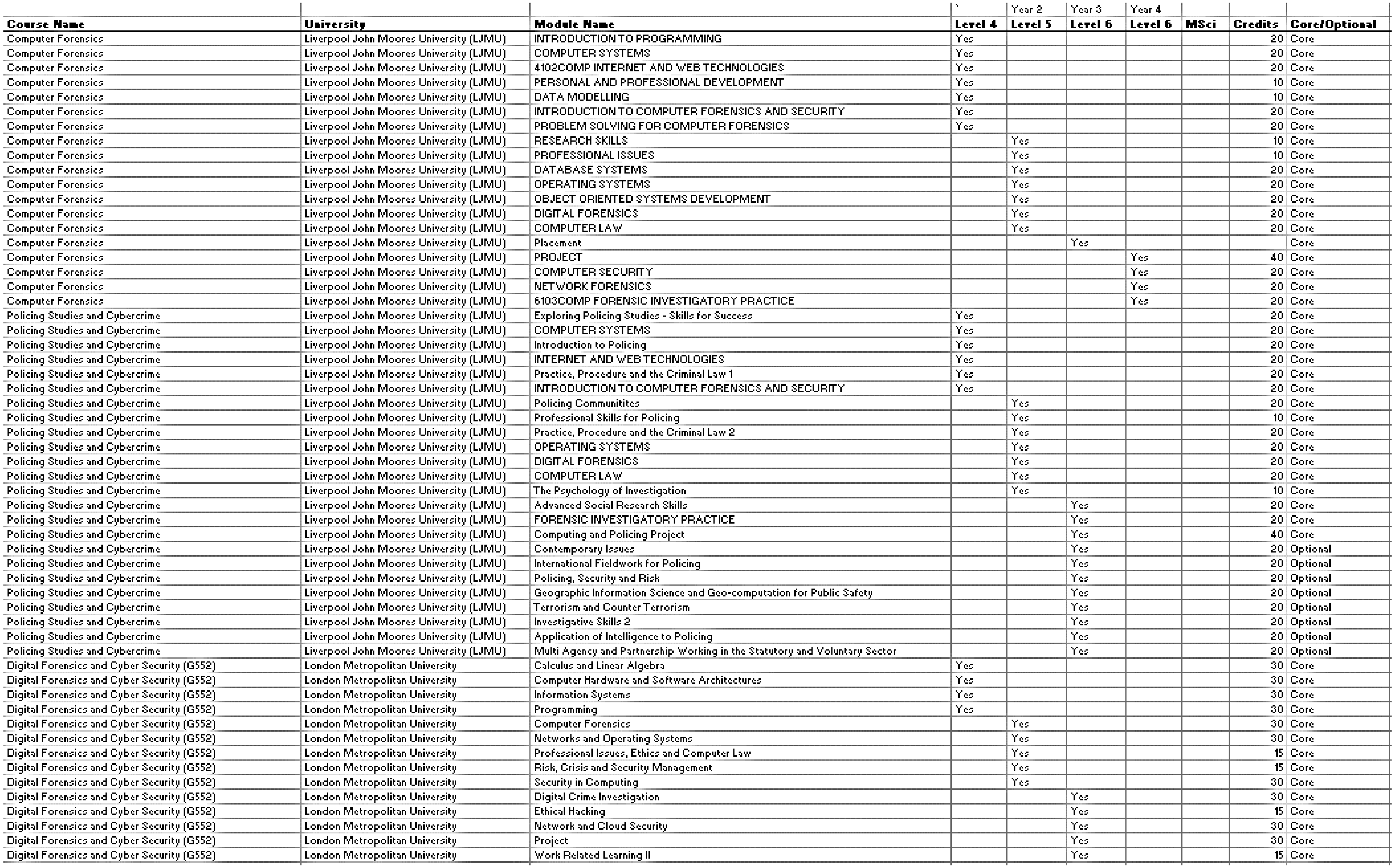
			`	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Computer Security and Forensics	University of Greenwich	Communication Systems	Yes					15	Core
Computer Security and Forensics	University of Greenwich	Computer Systems Architectures	Yes					15	Core
Computer Security and Forensics	University of Greenwich	System Development	Yes					15	Core
Computer Security and Forensics	University of Greenwich	Scholarly and Acadmic Practice	Yes					15	Core
Computer Security and Forensics	University of Greenwich	Object Oriented Programming	Yes					15	Core
Computer Security and Forensics	University of Greenwich	Programming Foundations	Yes					15	Core
Computer Security and Forensics	University of Greenwich	Logical Foundations	Yes					15	Core
Computer Security and Forensics	University of Greenwich	Analytical Methods for Computing	Yes					15	Core
Computer Security and Forensics	University of Greenwich	Computer Forensics 2		Yes				15	Core
Computer Security and Forensics	University of Greenwich	Network Theory & Technologies		Yes				15	Core
Computer Security and Forensics	University of Greenwich	Network Security		Yes				15	Core
Computer Security and Forensics	University of Greenwich	Operating Systems		Yes				15	Core
Computer Security and Forensics	University of Greenwich	Systems Development Project		Yes				30	Core
Computer Security and Forensics	University of Greenwich	Professionalism in the IT Industry		Yes				15	Core
Computer Security and Forensics	University of Greenwich	Introduction to Smart Systems		Yes				15	Core
Computer Security and Forensics	University of Greenwich	Placement (Year)			Yes				Optional
Computer Security and Forensics	University of Greenwich	Computer Forensics 3				Yes		30	Core
Computer Security and Forensics	University of Greenwich	Project (CIS)				Yes		60	Core
Computer Security and Forensics	University of Greenwich	Smart Systems Development				Yes		15	Optional
Computer Security and Forensics	University of Greenwich	Network Technology				Yes		15	Optional
Computer Security and Forensics	University of Greenwich	Network Design and Implementation				Yes		15	Optional
Computer Security and Forensics	University of Greenwich	Penetration Testing and Ethical Vulnerability Scanning				Yes		15	Optional
Computer Security and Forensics	University of Greenwich	Web Application Development				Yes		15	Optional
Computer Security and Forensics	University of Greenwich	Programming Distributed Components				Yes		15	Optional
Computer Security and Forensics	University of Greenwich	Enterprise Server Management and Security				Yes		15	Optional
Computer Security and Forensics	University of Greenwich	Computing Education Placement				Yes		15	Optional
Cyber Security & Computer Forensics with Business	Kingston	Programming 1	Yes					30	Core
Cyber Security & Computer Forensics with Business	Kingston	IT Toolbox	Yes					30	Core
Cyber Security & Computer Forensics with Business	Kingston	Digital Forensics: Principles and Practices	Yes					30	Core
Cyber Security & Computer Forensics with Business	Kingston	Business Management	Yes					30	Core
Cyber Security & Computer Forensics with Business	Kingston	Computer Forensics and Ethical Hacking		Yes				30	Core
Cyber Security & Computer Forensics with Business	Kingston	Networking Concepts		Yes				30	Core
Cyber Security & Computer Forensics with Business	Kingston	Database and UML Modelling		Yes				30	Core
Cyber Security & Computer Forensics with Business	Kingston	Managing Resources		Yes				30	Core
Cyber Security & Computer Forensics with Business	Kingston	Placement (Year)			Yes				Optional
Cyber Security & Computer Forensics with Business	Kingston	Individual Project				Yes		30	Core
Cyber Security & Computer Forensics with Business	Kingston	Internet Security				Yes		30	Core
Cyber Security & Computer Forensics with Business	Kingston	Live and Network Forensics				Yes		30	Core
Cyber Security & Computer Forensics with Business	Kingston	Management Strategy and Operations				Yes		30	Core

Figure C.1.7 Course offerings by university and level of study



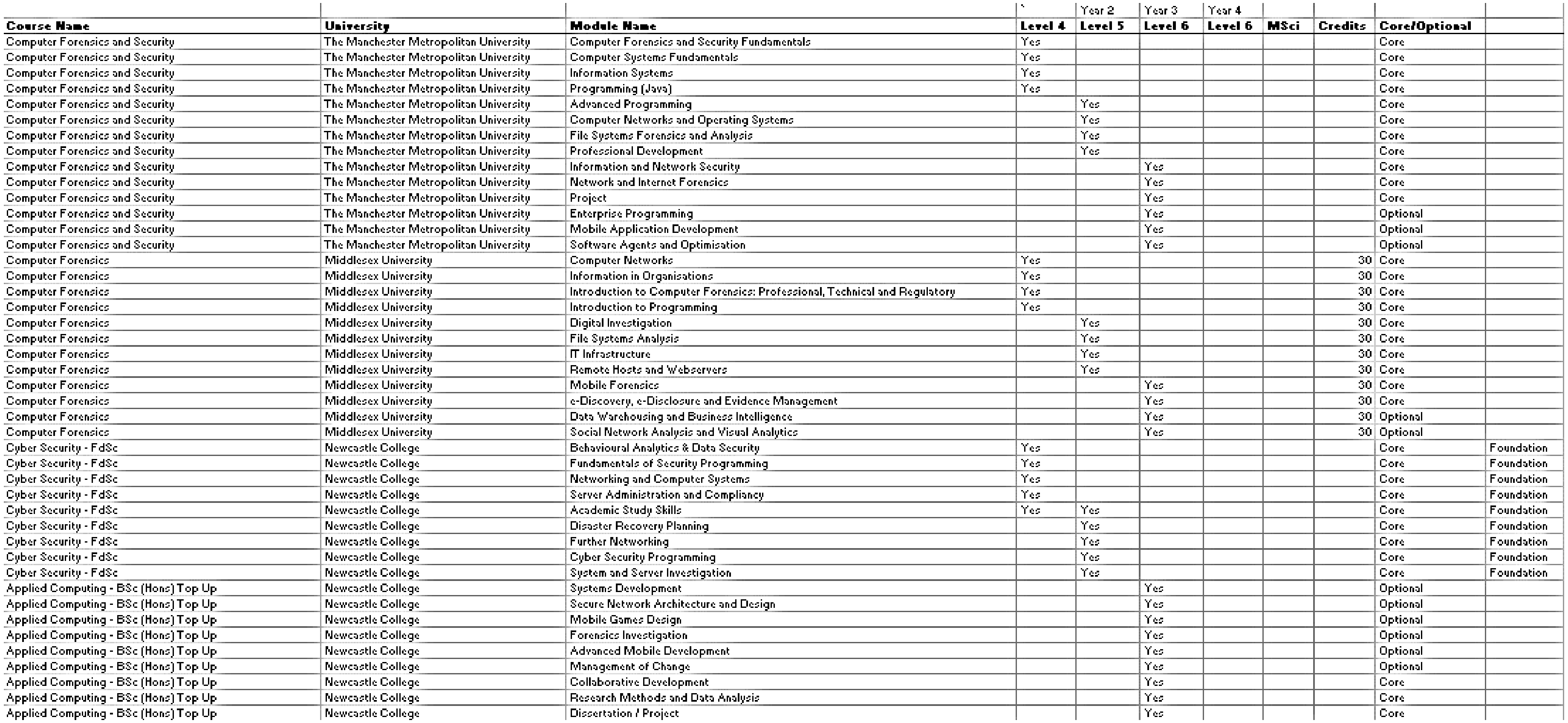
			`	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Computer Forensics	Leeds Beckett University	Fundamentals of Computer Programming	Yes					20	Core
Computer Forensics	Leeds Beckett University	Computer Communications	Yes					20	Core
Computer Forensics	Leeds Beckett University	Forensics & Security	Yes					20	Core
Computer Forensics	Leeds Beckett University	Object Oriented Programming	Yes					20	Core
Computer Forensics	Leeds Beckett University	Fundamentals of Databases	Yes					20	Core
Computer Forensics	Leeds Beckett University	Website Development	Yes					20	Core
Computer Forensics	Leeds Beckett University	Web & Network Security		Yes					Core
Computer Forensics	Leeds Beckett University	Team Project		Yes					Core
Computer Forensics	Leeds Beckett University	Digital Security Landscapes		Yes					Core
Computer Forensics	Leeds Beckett University	Digital Forensic Analysis		Yes					Core
Computer Forensics	Leeds Beckett University	Computer Forensic Processing		Yes					Core
Computer Forensics	Leeds Beckett University	Software Systems Development		Yes					Optional
Computer Forensics	Leeds Beckett University	Web Application Technologies		Yes					Optional
Computer Forensics	Leeds Beckett University	Database Systems		Yes					Optional
Computer Forensics	Leeds Beckett University	Placement			Yes				Optional
Computer Forensics	Leeds Beckett University	Forensic Investigation Techniques				Yes		20	Core
Computer Forensics	Leeds Beckett University	Networked Forensic Investigations				Yes		20	Core
Computer Forensics	Leeds Beckett University	Product Project				Yes		40	Core
Computer Forensics	Leeds Beckett University	Advanced Database Systems				Yes		20	Optional
Computer Forensics	Leeds Beckett University	Advanced Web Engineering				Yes		20	Optional
Computer Forensics	Leeds Beckett University	Advanced Software Engineering				Yes		20	Optional
Computer Forensics	Leeds Beckett University	Developing Mobile Applications				Yes		20	Optional
Computer Forensics	Leeds Beckett University	Human Computer Applications				Yes		20	Optional
Computer Forensics	Leeds Beckett University	Green Computing Technologies				Yes		20	Optional
Computer Forensics	Leeds Beckett University	Intelligent Systems				Yes		20	Optional
Computer Forensics and Security	Leeds Beckett University	Fundamentals of Computer Programming	Yes					20	Core
Computer Forensics and Security	Leeds Beckett University	Object Oriented Programming	Yes					20	Core
Computer Forensics and Security	Leeds Beckett University	Forensics & Security	Yes					20	Core
Computer Forensics and Security	Leeds Beckett University	Fundamentals of Databases	Yes					20	Core
Computer Forensics and Security	Leeds Beckett University	Website Development	Yes					20	Core
Computer Forensics and Security	Leeds Beckett University	Computer Communications	Yes					20	Core
Computer Forensics and Security	Leeds Beckett University	Computer Forensic Processing		Yes					Core
Computer Forensics and Security	Leeds Beckett University	Web & Network Security		Yes					Core
Computer Forensics and Security	Leeds Beckett University	Digital Security Landscapes		Yes					Core
Computer Forensics and Security	Leeds Beckett University	Digital Forensic Analysis		Yes					Core
Computer Forensics and Security	Leeds Beckett University	Team Project		Yes					Core
Computer Forensics and Security	Leeds Beckett University	Software Systems Development		Yes					Optional
Computer Forensics and Security	Leeds Beckett University	Web Application Technologies		Yes					Optional
Computer Forensics and Security	Leeds Beckett University	Database Systems		Yes					Optional
Computer Forensics and Security	Leeds Beckett University	Placement (Year)			Yes				Optional
Computer Forensics and Security	Leeds Beckett University	Advanced Digital Security				Yes			Core
Computer Forensics and Security	Leeds Beckett University	Networked Forensic Investigations				Yes			Core
Computer Forensics and Security	Leeds Beckett University	Production Project				Yes			Core
Computer Forensics and Security	Leeds Beckett University	Forensic Investigative Techniques				Yes			Optional
Computer Forensics and Security	Leeds Beckett University	Incident Response & Investigation				Yes			Optional
Computer Forensics and Security	Leeds Beckett University	Advanced Database Systems				Yes			Optiional
Computer Forensics and Security	Leeds Beckett University	Advanced Web Engineering				Yes			Optional
Computer Forensics and Security	Leeds Beckett University	Advanced Software Engineering				Yes			Optional

Figure C.1.8 Course offerings by university and level of study



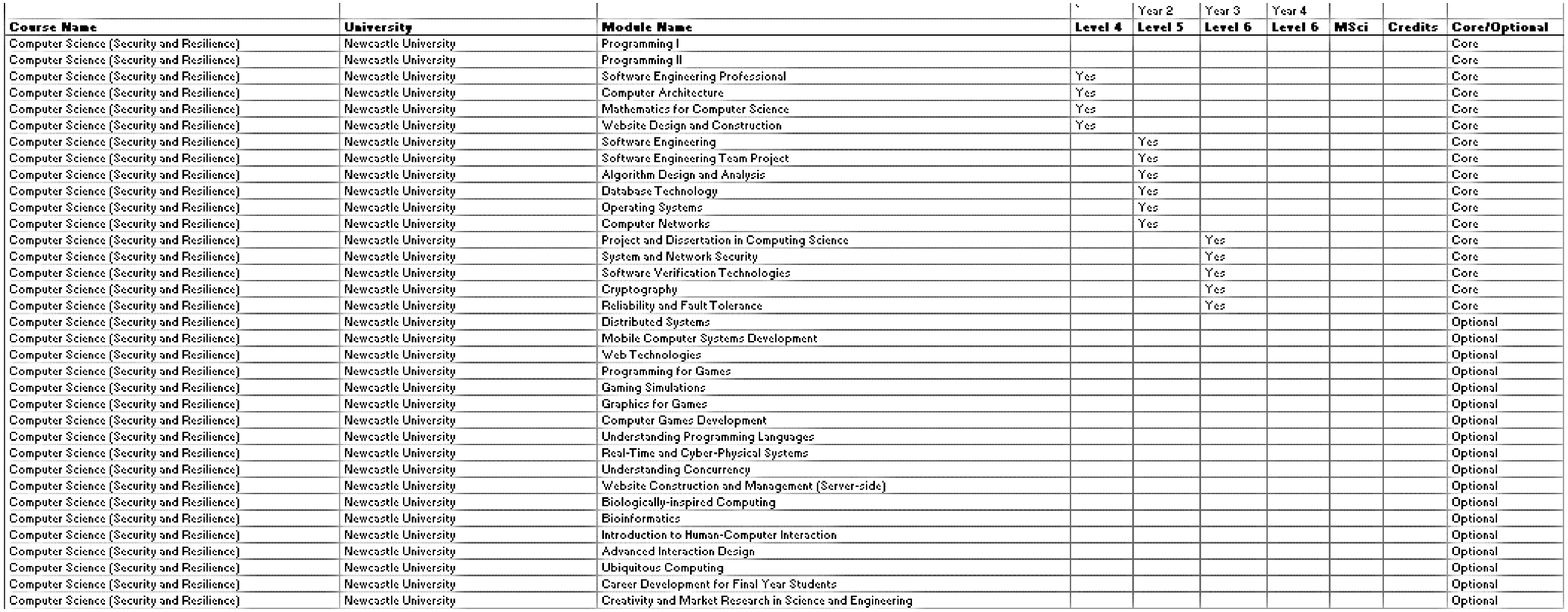
			`	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Computer Forensics	Liverpool John Moores University (LJMU)	INTRODUCTION TO PROGRAMMING	Yes					20	Core
Computer Forensics	Liverpool John Moores University (LJMU)	COMPUTER SYSTEMS	Yes					20	Core
Computer Forensics	Liverpool John Moores University (LJMU)	4102COMP INTERNET AND WEB TECHNOLOGIES	Yes					20	Core
Computer Forensics	Liverpool John Moores University (LJMU)	PERSONAL AND PROFESSIONAL DEVELOPMENT	Yes					10	Core
Computer Forensics	Liverpool John Moores University (LJMU)	DATA MODELLING	Yes					10	Core
Computer Forensics	Liverpool John Moores University (LJMU)	INTRODUCTION TO COMPUTER FORENSICS AND SECURITY	Yes					20	Core
Computer Forensics	Liverpool John Moores University (LJMU)	PROBLEM SOLVING FOR COMPUTER FORENSICS	Yes					20	Core
Computer Forensics	Liverpool John Moores University (LJMU)	RESEARCH SKILLS		Yes				10	Core
Computer Forensics	Liverpool John Moores University (LJMU)	PROFESSIONAL ISSUES		Yes				10	Core
Computer Forensics	Liverpool John Moores University (LJMU)	DATABASE SYSTEMS		Yes				20	Core
Computer Forensics	Liverpool John Moores University (LJMU)	OPERATING SYSTEMS		Yes				20	Core
Computer Forensics	Liverpool John Moores University (LJMU)	OBJECT ORIENTED SYSTEMS DEVELOPMENT		Yes				20	Core
Computer Forensics	Liverpool John Moores University (LJMU)	DIGITAL FORENSICS		Yes				20	Core
Computer Forensics	Liverpool John Moores University (LJMU)	COMPUTER LAW		Yes				20	Core
Computer Forensics	Liverpool John Moores University (LJMU)	Placement			Yes				Core
Computer Forensics	Liverpool John Moores University (LJMU)	PROJECT				Yes		40	Core
Computer Forensics	Liverpool John Moores University (LJMU)	COMPUTER SECURITY				Yes		20	Core
Computer Forensics	Liverpool John Moores University (LJMU)	NETWORK FORENSICS				Yes		20	Core
Computer Forensics	Liverpool John Moores University (LJMU)	6103COMP FORENSIC INVESTIGATORY PRACTICE				Yes		20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Exploring Policing Studies - Skills for Success	Yes					20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	COMPUTER SYSTEMS	Yes					20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Introduction to Policing	Yes					20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	INTERNET AND WEB TECHNOLOGIES	Yes					20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Practice, Procedure and the Criminal Law 1	Yes					20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	INTRODUCTION TO COMPUTER FORENSICS AND SECURITY	Yes					20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Policing Communitites		Yes				20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Professional Skills for Policing		Yes				10	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Practice, Procedure and the Criminal Law 2		Yes				20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	OPERATING SYSTEMS		Yes				20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	DIGITAL FORENSICS		Yes				20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	COMPUTER LAW		Yes				20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	The Psychology of Investigation		Yes				10	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Advanced Social Research Skills			Yes			20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	FORENSIC INVESTIGATORY PRACTICE			Yes			20	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Computing and Policing Project			Yes			40	Core
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Contemporary Issues			Yes			20	Optional
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	International Fieldwork for Policing			Yes			20	Optional
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Policing, Security and Risk			Yes			20	Optional
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Geographic Information Science and Geo-computation for Public Safety			Yes			20	Optional
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Terrorism and Counter Terrorism			Yes			20	Optional
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Investigative Skills 2			Yes			20	Optional
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Application of Intelligence to Policing			Yes			20	Optional
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)	Multi Agency and Partnership Working in the Statutory and Voluntary Sector			Yes			20	Optional
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Calculus and Linear Algebra	Yes					30	Core
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Computer Hardware and Software Architectures	Yes					30	Core
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Information Systems	Yes					30	Core
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Programming	Yes					30	Core
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Computer Forensics		Yes				30	Core
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Networks and Operating Systems		Yes				30	Core
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Professional Issues, Ethics and Computer Law		Yes				15	Core
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Risk, Crisis and Security Management		Yes				15	Core
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Security in Computing		Yes				30	Core
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Digital Crime Investigation			Yes			30	Core
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Ethical Hacking			Yes			15	Core
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Network and Cloud Security			Yes			30	Core
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Project			Yes			30	Core
Digital Forensics and Cyber Security (G552)	London Metropolitan University	Work Related Learning II			Yes			15	Core

Figure C.1.9 Course offerings by university and level of study



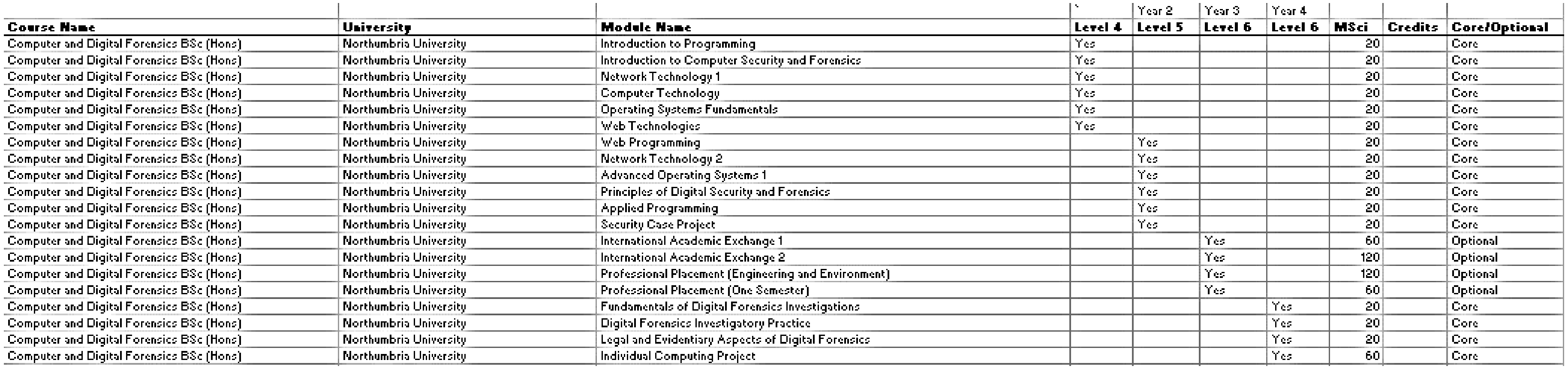
			`	Year 2	Year 3	Year 4				
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**	
Computer Forensics and Security	The Manchester Metropolitan University	Computer Forensics and Security Fundamentals	Yes						Core	
Computer Forensics and Security	The Manchester Metropolitan University	Computer Systems Fundamentals	Yes						Core	
Computer Forensics and Security	The Manchester Metropolitan University	Information Systems	Yes						Core	
Computer Forensics and Security	The Manchester Metropolitan University	Programming (Java)	Yes						Core	
Computer Forensics and Security	The Manchester Metropolitan University	Advanced Programming		Yes					Core	
Computer Forensics and Security	The Manchester Metropolitan University	Computer Networks and Operating Systems		Yes					Core	
Computer Forensics and Security	The Manchester Metropolitan University	File Systems Forensics and Analysis		Yes					Core	
Computer Forensics and Security	The Manchester Metropolitan University	Professional Development		Yes					Core	
Computer Forensics and Security	The Manchester Metropolitan University	Information and Network Security			Yes				Core	
Computer Forensics and Security	The Manchester Metropolitan University	Network and Internet Forensics			Yes				Core	
Computer Forensics and Security	The Manchester Metropolitan University	Project			Yes				Core	
Computer Forensics and Security	The Manchester Metropolitan University	Enterprise Programming			Yes				Optional	
Computer Forensics and Security	The Manchester Metropolitan University	Mobile Application Development			Yes				Optional	
Computer Forensics and Security	The Manchester Metropolitan University	Software Agents and Optimisation			Yes				Optional	
Computer Forensics	Middlesex University	Computer Networks	Yes					30	Core	
Computer Forensics	Middlesex University	Information in Organisations	Yes					30	Core	
Computer Forensics	Middlesex University	Introduction to Computer Forensics: Professional, Technical and Regulatory	Yes					30	Core	
Computer Forensics	Middlesex University	Introduction to Programming	Yes					30	Core	
Computer Forensics	Middlesex University	Digital Investigation		Yes				30	Core	
Computer Forensics	Middlesex University	File Systems Analysis		Yes				30	Core	
Computer Forensics	Middlesex University	IT Infrastructure		Yes				30	Core	
Computer Forensics	Middlesex University	Remote Hosts and Webservers		Yes				30	Core	
Computer Forensics	Middlesex University	Mobile Forensics			Yes			30	Core	
Computer Forensics	Middlesex University	e-Discovery, e-Disclosure and Evidence Management			Yes			30	Core	
Computer Forensics	Middlesex University	Data Warehousing and Business Intelligence			Yes			30	Optional	
Computer Forensics	Middlesex University	Social Network Analysis and Visual Analytics			Yes			30	Optional	
Cyber Security - FdSc	Newcastle College	Behavioural Analytics & Data Security	Yes						Core	Foundation
Cyber Security - FdSc	Newcastle College	Fundamentals of Security Programming	Yes						Core	Foundation
Cyber Security - FdSc	Newcastle College	Networking and Computer Systems	Yes						Core	Foundation
Cyber Security - FdSc	Newcastle College	Server Administration and Compliancy	Yes						Core	Foundation
Cyber Security - FdSc	Newcastle College	Academic Study Skills	Yes	Yes					Core	Foundation
Cyber Security - FdSc	Newcastle College	Disaster Recovery Planning		Yes					Core	Foundation
Cyber Security - FdSc	Newcastle College	Further Networking		Yes					Core	Foundation
Cyber Security - FdSc	Newcastle College	Cyber Security Programming		Yes					Core	Foundation
Cyber Security - FdSc	Newcastle College	System and Server Investigation		Yes					Core	Foundation
Applied Computing - BSc (Hons) Top Up	Newcastle College	Systems Development			Yes				Optional	
Applied Computing - BSc (Hons) Top Up	Newcastle College	Secure Network Architecture and Design			Yes				Optional	
Applied Computing - BSc (Hons) Top Up	Newcastle College	Mobile Games Design			Yes				Optional	
Applied Computing - BSc (Hons) Top Up	Newcastle College	Forensics Investigation			Yes				Optional	
Applied Computing - BSc (Hons) Top Up	Newcastle College	Advanced Mobile Development			Yes				Optional	
Applied Computing - BSc (Hons) Top Up	Newcastle College	Management of Change			Yes				Optional	
Applied Computing - BSc (Hons) Top Up	Newcastle College	Collaborative Development			Yes				Core	
Applied Computing - BSc (Hons) Top Up	Newcastle College	Research Methods and Data Analysis			Yes				Core	
Applied Computing - BSc (Hons) Top Up	Newcastle College	Dissertation / Project			Yes				Core	

Figure C.1.10 Course offerings by university and level of study



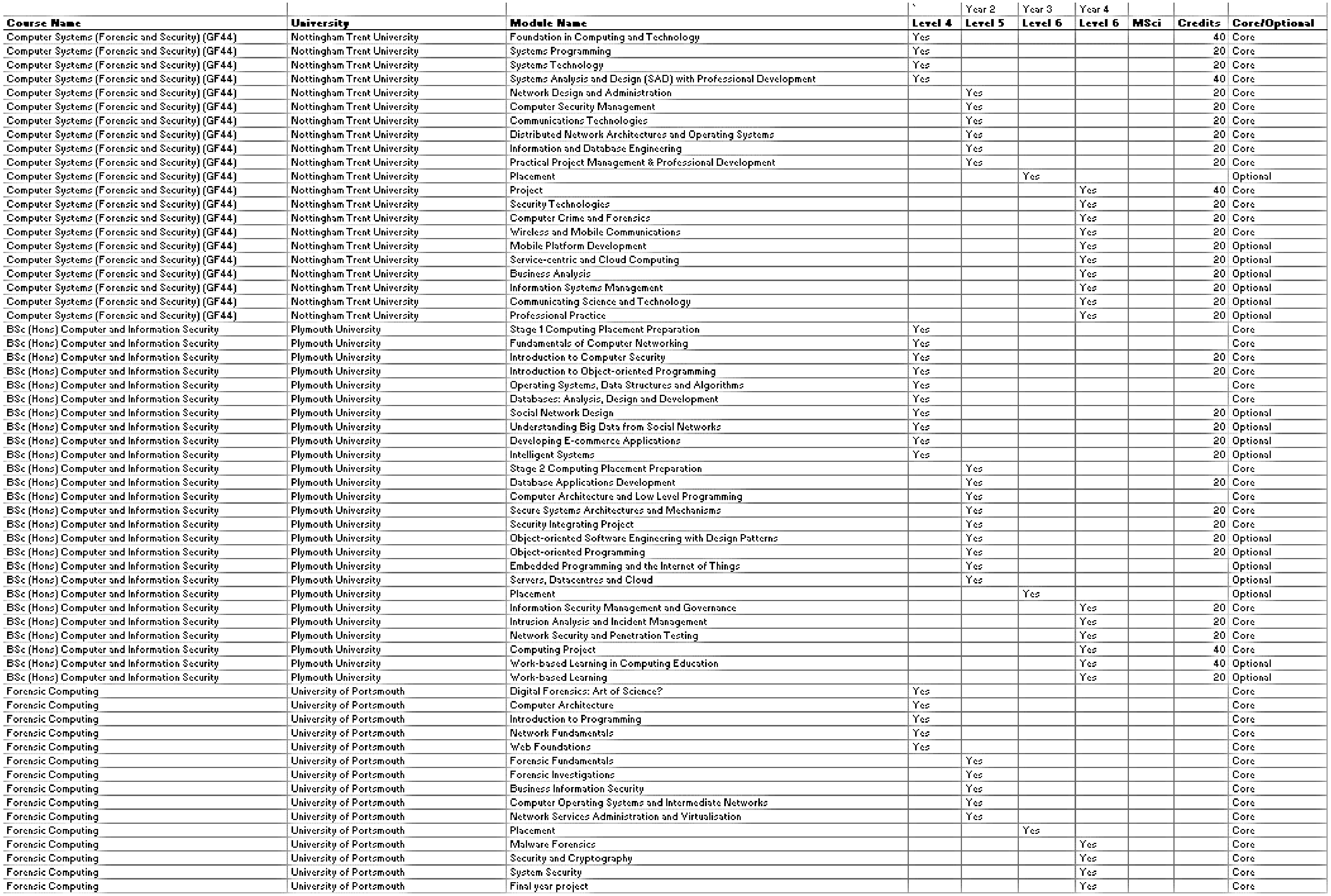
			`	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Computer Science (Security and Resilience)	Newcastle University	Programming I							Core
Computer Science (Security and Resilience)	Newcastle University	Programming II							Core
Computer Science (Security and Resilience)	Newcastle University	Software Engineering Professional	Yes						Core
Computer Science (Security and Resilience)	Newcastle University	Computer Architecture	Yes						Core
Computer Science (Security and Resilience)	Newcastle University	Mathematics for Computer Science	Yes						Core
Computer Science (Security and Resilience)	Newcastle University	Website Design and Construction	Yes						Core
Computer Science (Security and Resilience)	Newcastle University	Software Engineering		Yes					Core
Computer Science (Security and Resilience)	Newcastle University	Software Engineering Team Project		Yes					Core
Computer Science (Security and Resilience)	Newcastle University	Algorithm Design and Analysis		Yes					Core
Computer Science (Security and Resilience)	Newcastle University	Database Technology		Yes					Core
Computer Science (Security and Resilience)	Newcastle University	Operating Systems		Yes					Core
Computer Science (Security and Resilience)	Newcastle University	Computer Networks		Yes					Core
Computer Science (Security and Resilience)	Newcastle University	Project and Dissertation in Computing Science			Yes				Core
Computer Science (Security and Resilience)	Newcastle University	System and Network Security			Yes				Core
Computer Science (Security and Resilience)	Newcastle University	Software Verification Technologies			Yes				Core
Computer Science (Security and Resilience)	Newcastle University	Cryptography			Yes				Core
Computer Science (Security and Resilience)	Newcastle University	Reliability and Fault Tolerance			Yes				Core
Computer Science (Security and Resilience)	Newcastle University	Distributed Systems							Optional
Computer Science (Security and Resilience)	Newcastle University	Mobile Computer Systems Development							Optional
Computer Science (Security and Resilience)	Newcastle University	Web Technologies							Optional
Computer Science (Security and Resilience)	Newcastle University	Programming for Games							Optional
Computer Science (Security and Resilience)	Newcastle University	Gaming Simulations							Optional
Computer Science (Security and Resilience)	Newcastle University	Graphics for Games							Optional
Computer Science (Security and Resilience)	Newcastle University	Computer Games Development							Optional
Computer Science (Security and Resilience)	Newcastle University	Understanding Programming Languages							Optional
Computer Science (Security and Resilience)	Newcastle University	Real-Time and Cyber-Physical Systems							Optional
Computer Science (Security and Resilience)	Newcastle University	Understanding Concurrency							Optional
Computer Science (Security and Resilience)	Newcastle University	Website Construction and Management (Server-side)							Optional
Computer Science (Security and Resilience)	Newcastle University	Biologically-inspired Computing							Optional
Computer Science (Security and Resilience)	Newcastle University	Bioinformatics							Optional
Computer Science (Security and Resilience)	Newcastle University	Introduction to Human-Computer Interaction							Optional
Computer Science (Security and Resilience)	Newcastle University	Advanced Interaction Design							Optional
Computer Science (Security and Resilience)	Newcastle University	Ubiquitous Computing							Optional
Computer Science (Security and Resilience)	Newcastle University	Career Development for Final Year Students							Optional
Computer Science (Security and Resilience)	Newcastle University	Creativity and Market Research in Science and Engineering							Optional

Figure C.1.11 Course offerings by university and level of study



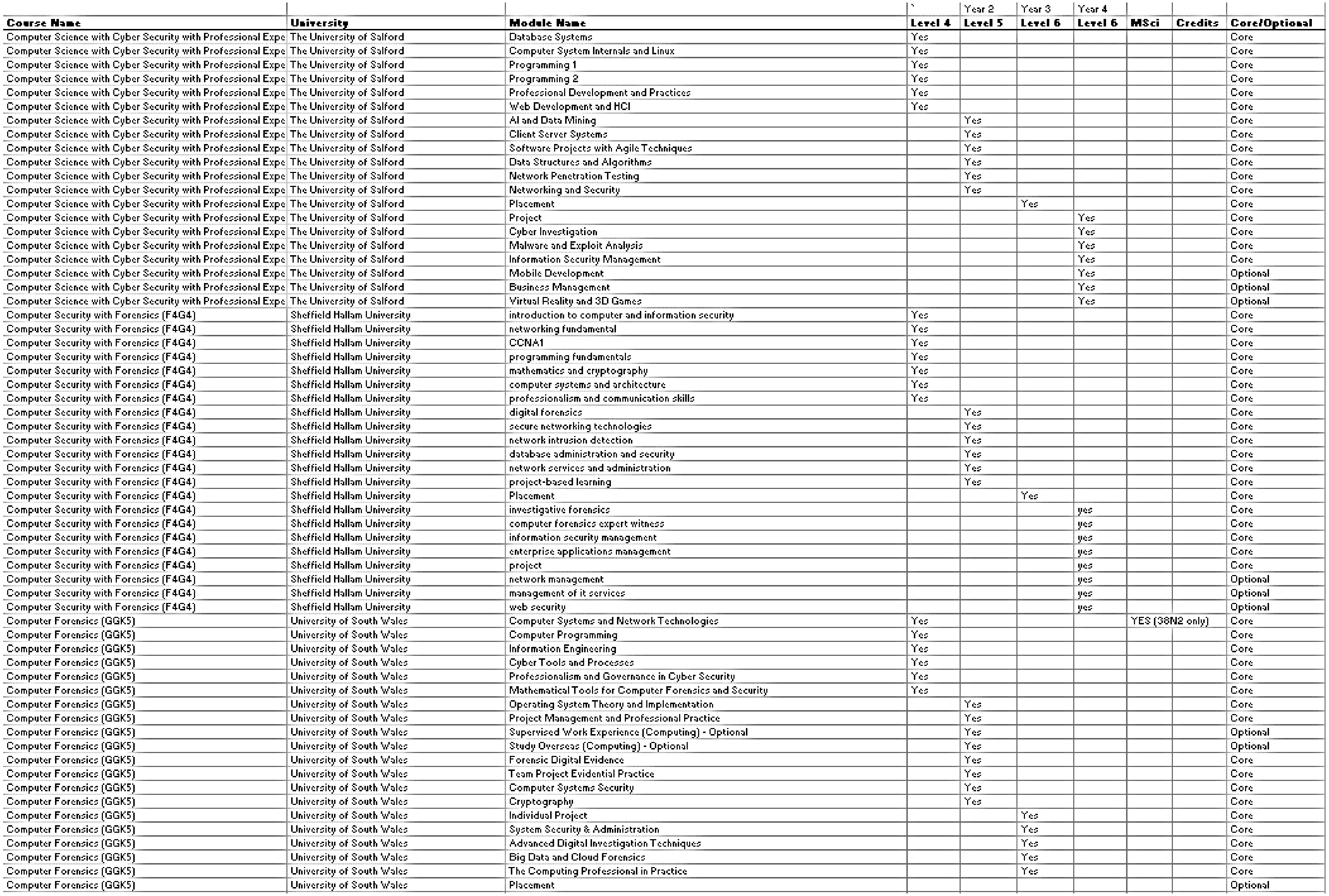
			`	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Computer and Digital Forensics BSc (Hons)	Northumbria University	Introduction to Programming	Yes				20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Introduction to Computer Security and Forensics	Yes				20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Network Technology 1	Yes				20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Computer Technology	Yes				20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Operating Systems Fundamentals	Yes				20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Web Technologies	Yes				20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Web Programming		Yes			20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Network Technology 2		Yes			20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Advanced Operating Systems 1		Yes			20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Principles of Digital Security and Forensics		Yes			20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Applied Programming		Yes			20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Security Case Project		Yes			20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	International Academic Exchange 1			Yes		60		Optional
Computer and Digital Forensics BSc (Hons)	Northumbria University	International Academic Exchange 2			Yes		120		Optional
Computer and Digital Forensics BSc (Hons)	Northumbria University	Professional Placement (Engineering and Environment)			Yes		120		Optional
Computer and Digital Forensics BSc (Hons)	Northumbria University	Professional Placement (One Semester)			Yes		60		Optional
Computer and Digital Forensics BSc (Hons)	Northumbria University	Fundamentals of Digital Forensics Investigations				Yes	20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Digital Forensics Investigatory Practice				Yes	20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Legal and Evidentiary Aspects of Digital Forensics				Yes	20		Core
Computer and Digital Forensics BSc (Hons)	Northumbria University	Individual Computing Project				Yes	60		Core

Figure C.1.12 Course offerings by university and level of study



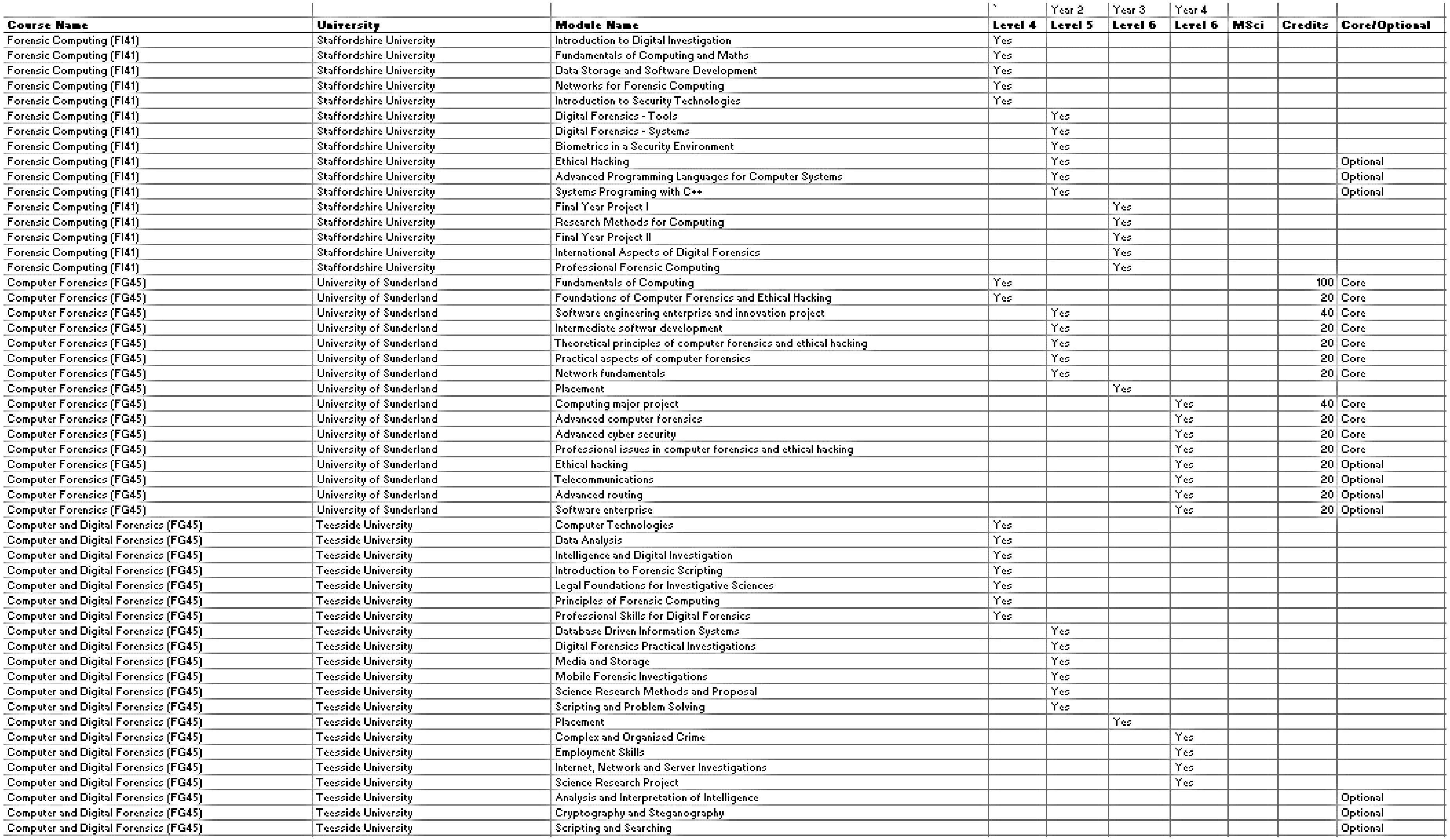
			`	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Foundation in Computing and Technology	Yes					40	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Systems Programming	Yes					20	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Systems Technology	Yes					20	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Systems Analysis and Design (SAD) with Professional Development	Yes					40	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Network Design and Administration		Yes				20	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Computer Security Management		Yes				20	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Communications Technologies		Yes				20	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Distributed Network Architectures and Operating Systems		Yes				20	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Information and Database Engineering		Yes				20	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Practical Project Management & Professional Development		Yes				20	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Placement			Yes				Optional
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Project				Yes		40	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Security Technologies				Yes		20	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Computer Crime and Forensics				Yes		20	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Wireless and Mobile Communications				Yes		20	Core
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Mobile Platform Development				Yes		20	Optional
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Service-centric and Cloud Computing				Yes		20	Optional
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Business Analysis				Yes		20	Optional
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Information Systems Management				Yes		20	Optional
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Communicating Science and Technology				Yes		20	Optional
Computer Systems (Forensic and Security) (GF44)	Nottingham Trent University	Professional Practice				Yes		20	Optional
BSc (Hons) Computer and Information Security	Plymouth University	Stage 1 Computing Placement Preparation	Yes						Core
BSc (Hons) Computer and Information Security	Plymouth University	Fundamentals of Computer Networking	Yes						Core
BSc (Hons) Computer and Information Security	Plymouth University	Introduction to Computer Security	Yes					20	Core
BSc (Hons) Computer and Information Security	Plymouth University	Introduction to Object-oriented Programming	Yes					20	Core
BSc (Hons) Computer and Information Security	Plymouth University	Operating Systems, Data Structures and Algorithms	Yes						Core
BSc (Hons) Computer and Information Security	Plymouth University	Databases: Analysis, Design and Development	Yes						Core
BSc (Hons) Computer and Information Security	Plymouth University	Social Network Design	Yes					20	Optional
BSc (Hons) Computer and Information Security	Plymouth University	Understanding Big Data from Social Networks	Yes					20	Optional
BSc (Hons) Computer and Information Security	Plymouth University	Developing E-commerce Applications	Yes					20	Optional
BSc (Hons) Computer and Information Security	Plymouth University	Intelligent Systems	Yes					20	Optional
BSc (Hons) Computer and Information Security	Plymouth University	Stage 2 Computing Placement Preparation		Yes					Core
BSc (Hons) Computer and Information Security	Plymouth University	Database Applications Development		Yes				20	Core
BSc (Hons) Computer and Information Security	Plymouth University	Computer Architecture and Low Level Programming		Yes					Core
BSc (Hons) Computer and Information Security	Plymouth University	Secure Systems Architectures and Mechanisms		Yes				20	Core
BSc (Hons) Computer and Information Security	Plymouth University	Security Integrating Project		Yes				20	Core
BSc (Hons) Computer and Information Security	Plymouth University	Object-oriented Software Engineering with Design Patterns		Yes				20	Optional
BSc (Hons) Computer and Information Security	Plymouth University	Object-oriented Programming		Yes				20	Optional
BSc (Hons) Computer and Information Security	Plymouth University	Embedded Programming and the Internet of Things		Yes					Optional
BSc (Hons) Computer and Information Security	Plymouth University	Servers, Datacentres and Cloud		Yes					Optional
BSc (Hons) Computer and Information Security	Plymouth University	Placement			Yes				Optional
BSc (Hons) Computer and Information Security	Plymouth University	Information Security Management and Governance				Yes		20	Core
BSc (Hons) Computer and Information Security	Plymouth University	Intrusion Analysis and Incident Management				Yes		20	Core
BSc (Hons) Computer and Information Security	Plymouth University	Network Security and Penetration Testing				Yes		20	Core
BSc (Hons) Computer and Information Security	Plymouth University	Computing Project				Yes		40	Core
BSc (Hons) Computer and Information Security	Plymouth University	Work-based Learning in Computing Education				Yes		40	Optional
BSc (Hons) Computer and Information Security	Plymouth University	Work-based Learning				Yes		20	Optional
Forensic Computing	University of Portsmouth	Digital Forensics: Art of Science?	Yes						Core
Forensic Computing	University of Portsmouth	Computer Architecture	Yes						Core
Forensic Computing	University of Portsmouth	Introduction to Programming	Yes						Core
Forensic Computing	University of Portsmouth	Network Fundamentals	Yes						Core
Forensic Computing	University of Portsmouth	Web Foundations	Yes						Core
Forensic Computing	University of Portsmouth	Forensic Fundamentals		Yes					Core
Forensic Computing	University of Portsmouth	Forensic Investigations		Yes					Core
Forensic Computing	University of Portsmouth	Business Information Security		Yes					Core
Forensic Computing	University of Portsmouth	Computer Operating Systems and Intermediate Networks		Yes					Core
Forensic Computing	University of Portsmouth	Network Services Administration and Virtualisation		Yes					Core
Forensic Computing	University of Portsmouth	Placement			Yes				Core
Forensic Computing	University of Portsmouth	Malware Forensics				Yes			Core
Forensic Computing	University of Portsmouth	Security and Cryptography				Yes			Core
Forensic Computing	University of Portsmouth	System Security				Yes			Core
Forensic Computing	University of Portsmouth	Final year project				Yes			Core

Figure C.1.13 Course offerings by university and level of study



			`	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Computer Science with Cyber Security with Professional Expe	The University of Salford	Database Systems	Yes						Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Computer System Internals and Linux	Yes						Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Programming 1	Yes						Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Programming 2	Yes						Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Professional Development and Practices	Yes						Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Web Development and HCI	Yes						Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	AI and Data Mining		Yes					Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Client Server Systems		Yes					Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Software Projects with Agile Techniques		Yes					Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Data Structures and Algorithms		Yes					Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Network Penetration Testing		Yes					Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Networking and Security		Yes					Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Placement			Yes				Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Project				Yes			Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Cyber Investigation				Yes			Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Malware and Exploit Analysis				Yes			Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Information Security Management				Yes			Core
Computer Science with Cyber Security with Professional Expe	The University of Salford	Mobile Development				Yes			Optional
Computer Science with Cyber Security with Professional Expe	The University of Salford	Business Management				Yes			Optional
Computer Science with Cyber Security with Professional Expe	The University of Salford	Virtual Reality and 3D Games				Yes			Optional
Computer Security with Forensics (F4G4)	Sheffield Hallam University	introduction to computer and information security	Yes						Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	networking fundamental	Yes						Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	CCNA1	Yes						Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	programming fundamentals	Yes						Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	mathematics and cryptography	Yes						Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	computer systems and architecture	Yes						Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	professionalism and communication skills	Yes						Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	digital forensics		Yes					Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	secure networking technologies		Yes					Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	network intrusion detection		Yes					Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	database administration and security		Yes					Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	network services and administration		Yes					Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	project-based learning		Yes					Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	Placement			Yes				Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	investigative forensics				yes			Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	computer forensics expert witness				yes			Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	information security management				yes			Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	enterprise applications management				yes			Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	project				yes			Core
Computer Security with Forensics (F4G4)	Sheffield Hallam University	network management				yes			Optional
Computer Security with Forensics (F4G4)	Sheffield Hallam University	management of it services				yes			Optional
Computer Security with Forensics (F4G4)	Sheffield Hallam University	web security				yes			Optional
Computer Forensics (GGK5)	University of South Wales	Computer Systems and Network Technologies	Yes				YES (38N2 only)		Core
Computer Forensics (GGK5)	University of South Wales	Computer Programming	Yes						Core
Computer Forensics (GGK5)	University of South Wales	Information Engineering	Yes						Core
Computer Forensics (GGK5)	University of South Wales	Cyber Tools and Processes	Yes						Core
Computer Forensics (GGK5)	University of South Wales	Professionalism and Governance in Cyber Security	Yes						Core
Computer Forensics (GGK5)	University of South Wales	Mathematical Tools for Computer Forensics and Security	Yes						Core
Computer Forensics (GGK5)	University of South Wales	Operating System Theory and Implementation		Yes					Core
Computer Forensics (GGK5)	University of South Wales	Project Management and Professional Practice		Yes					Core
Computer Forensics (GGK5)	University of South Wales	Supervised Work Experience (Computing) - Optional		Yes					Optional
Computer Forensics (GGK5)	University of South Wales	Study Overseas (Computing) - Optional		Yes					Optional
Computer Forensics (GGK5)	University of South Wales	Forensic Digital Evidence		Yes					Core
Computer Forensics (GGK5)	University of South Wales	Team Project Evidential Practice		Yes					Core
Computer Forensics (GGK5)	University of South Wales	Computer Systems Security		Yes					Core
Computer Forensics (GGK5)	University of South Wales	Cryptography		Yes					Core
Computer Forensics (GGK5)	University of South Wales	Individual Project			Yes				Core
Computer Forensics (GGK5)	University of South Wales	System Security & Administration			Yes				Core
Computer Forensics (GGK5)	University of South Wales	Advanced Digital Investigation Techniques			Yes				Core
Computer Forensics (GGK5)	University of South Wales	Big Data and Cloud Forensics			Yes				Core
Computer Forensics (GGK5)	University of South Wales	The Computing Professional in Practice			Yes				Core
Computer Forensics (GGK5)	University of South Wales	Placement							Optional

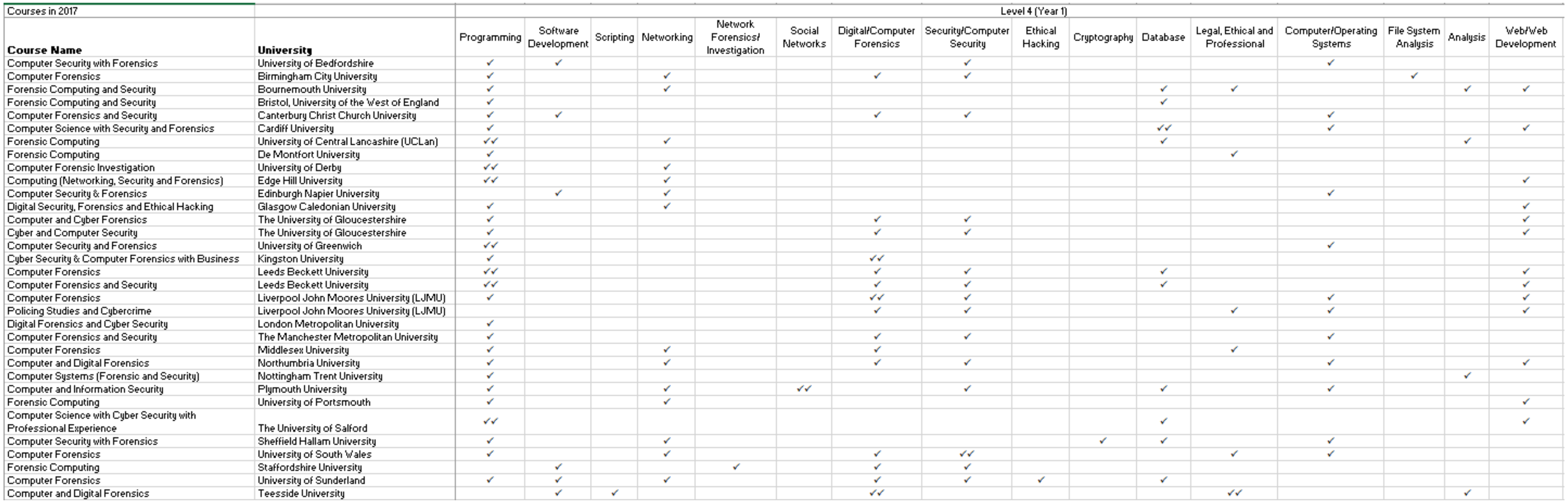
Figure C.1.14 Course offerings by university and level of study



			`	Year 2	Year 3	Year 4			
Course Name	**University**	**Module Name**	**Level 4**	**Level 5**	**Level 6**	**Level 6**	**MSci**	**Credits**	**Core/Optional**
Forensic Computing (FI41)	Staffordshire University	Introduction to Digital Investigation	Yes						
Forensic Computing (FI41)	Staffordshire University	Fundamentals of Computing and Maths	Yes						
Forensic Computing (FI41)	Staffordshire University	Data Storage and Software Development	Yes						
Forensic Computing (FI41)	Staffordshire University	Networks for Forensic Computing	Yes						
Forensic Computing (FI41)	Staffordshire University	Introduction to Security Technologies	Yes						
Forensic Computing (FI41)	Staffordshire University	Digital Forensics - Tools		Yes					
Forensic Computing (FI41)	Staffordshire University	Digital Forensics - Systems		Yes					
Forensic Computing (FI41)	Staffordshire University	Biometrics in a Security Environment		Yes					
Forensic Computing (FI41)	Staffordshire University	Ethical Hacking		Yes					Optional
Forensic Computing (FI41)	Staffordshire University	Advanced Programming Languages for Computer Systems		Yes					Optional
Forensic Computing (FI41)	Staffordshire University	Systems Programing with C++		Yes					Optional
Forensic Computing (FI41)	Staffordshire University	Final Year Project I			Yes				
Forensic Computing (FI41)	Staffordshire University	Research Methods for Computing			Yes				
Forensic Computing (FI41)	Staffordshire University	Final Year Project II			Yes				
Forensic Computing (FI41)	Staffordshire University	International Aspects of Digital Forensics			Yes				
Forensic Computing (FI41)	Staffordshire University	Professional Forensic Computing			Yes				
Computer Forensics (FG45)	University of Sunderland	Fundamentals of Computing	Yes					100	Core
Computer Forensics (FG45)	University of Sunderland	Foundations of Computer Forensics and Ethical Hacking	Yes					20	Core
Computer Forensics (FG45)	University of Sunderland	Software engineering enterprise and innovation project		Yes				40	Core
Computer Forensics (FG45)	University of Sunderland	Intermediate softwar development		Yes				20	Core
Computer Forensics (FG45)	University of Sunderland	Theoretical principles of computer forensics and ethical hacking		Yes				20	Core
Computer Forensics (FG45)	University of Sunderland	Practical aspects of computer forensics		Yes				20	Core
Computer Forensics (FG45)	University of Sunderland	Network fundamentals		Yes				20	Core
Computer Forensics (FG45)	University of Sunderland	Placement			Yes				
Computer Forensics (FG45)	University of Sunderland	Computing major project				Yes		40	Core
Computer Forensics (FG45)	University of Sunderland	Advanced computer forensics				Yes		20	Core
Computer Forensics (FG45)	University of Sunderland	Advanced cyber security				Yes		20	Core
Computer Forensics (FG45)	University of Sunderland	Professional issues in computer forensics and ethical hacking				Yes		20	Core
Computer Forensics (FG45)	University of Sunderland	Ethical hacking				Yes		20	Optional
Computer Forensics (FG45)	University of Sunderland	Telecommunications				Yes		20	Optional
Computer Forensics (FG45)	University of Sunderland	Advanced routing				Yes		20	Optional
Computer Forensics (FG45)	University of Sunderland	Software enterprise				Yes		20	Optional
Computer and Digital Forensics (FG45)	Teesside University	Computer Technologies	Yes						
Computer and Digital Forensics (FG45)	Teesside University	Data Analysis	Yes						
Computer and Digital Forensics (FG45)	Teesside University	Intelligence and Digital Investigation	Yes						
Computer and Digital Forensics (FG45)	Teesside University	Introduction to Forensic Scripting	Yes						
Computer and Digital Forensics (FG45)	Teesside University	Legal Foundations for Investigative Sciences	Yes						
Computer and Digital Forensics (FG45)	Teesside University	Principles of Forensic Computing	Yes						
Computer and Digital Forensics (FG45)	Teesside University	Professional Skills for Digital Forensics	Yes						
Computer and Digital Forensics (FG45)	Teesside University	Database Driven Information Systems		Yes					
Computer and Digital Forensics (FG45)	Teesside University	Digital Forensics Practical Investigations		Yes					
Computer and Digital Forensics (FG45)	Teesside University	Media and Storage		Yes					
Computer and Digital Forensics (FG45)	Teesside University	Mobile Forensic Investigations		Yes					
Computer and Digital Forensics (FG45)	Teesside University	Science Research Methods and Proposal		Yes					
Computer and Digital Forensics (FG45)	Teesside University	Scripting and Problem Solving		Yes					
Computer and Digital Forensics (FG45)	Teesside University	Placement			Yes				
Computer and Digital Forensics (FG45)	Teesside University	Complex and Organised Crime				Yes			
Computer and Digital Forensics (FG45)	Teesside University	Employment Skills				Yes			
Computer and Digital Forensics (FG45)	Teesside University	Internet, Network and Server Investigations				Yes			
Computer and Digital Forensics (FG45)	Teesside University	Science Research Project				Yes			
Computer and Digital Forensics (FG45)	Teesside University	Analysis and Interpretation of Intelligence							Optional
Computer and Digital Forensics (FG45)	Teesside University	Cryptography and Steganography							Optional
Computer and Digital Forensics (FG45)	Teesside University	Scripting and Searching							Optional

Figure C.1.15 Course offerings by university and level of study

C.2 Level 4 Course Offerings by Topics



Courses in 2017		Level 4 (Year 1)															
Course Name	**University**	Programming	Software Development	Scripting	Networking	Network Forensics/ Investigation	Social Networks	Digital/Computer Forensics	Security/Computer Security	Ethical Hacking	Cryptography	Database	Legal, Ethical and Professional	Computer/Operating Systems	File System Analysis	Analysis	Web/Web Development
Computer Security with Forensics	University of Bedfordshire	✓	✓						✓					✓			
Computer Forensics	Birmingham City University	✓			✓			✓	✓						✓		
Forensic Computing and Security	Bournemouth University	✓			✓							✓	✓			✓	✓
Forensic Computing and Security	Bristol, University of the West of England	✓										✓					
Computer Forensics and Security	Canterbury Christ Church University	✓	✓					✓	✓					✓			
Computer Science with Security and Forensics	Cardiff University	✓										✓✓		✓			✓
Forensic Computing	University of Central Lancashire (UCLan)	✓✓			✓							✓				✓	
Forensic Computing	De Montfort University	✓											✓				
Computer Forensic Investigation	University of Derby	✓✓			✓												
Computing (Networking, Security and Forensics)	Edge Hill University	✓✓			✓												✓
Computer Security & Forensics	Edinburgh Napier University		✓		✓									✓			
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	✓			✓												✓
Computer and Cyber Forensics	The University of Gloucestershire	✓						✓	✓								✓
Cyber and Computer Security	The University of Gloucestershire	✓						✓	✓								✓
Computer Security and Forensics	University of Greenwich	✓✓												✓			
Cyber Security & Computer Forensics with Business	Kingston University	✓						✓✓									
Computer Forensics	Leeds Beckett University	✓✓						✓	✓			✓					✓
Computer Forensics and Security	Leeds Beckett University	✓✓						✓	✓			✓					✓
Computer Forensics	Liverpool John Moores University (LJMU)	✓						✓✓	✓					✓			✓
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)							✓	✓				✓	✓			✓
Digital Forensics and Cyber Security	London Metropolitan University	✓															
Computer Forensics and Security	The Manchester Metropolitan University	✓						✓	✓					✓			
Computer Forensics	Middlesex University	✓			✓			✓					✓				
Computer and Digital Forensics	Northumbria University	✓			✓			✓	✓					✓			✓
Computer Systems (Forensic and Security)	Nottingham Trent University	✓														✓	
Computer and Information Security	Plymouth University	✓			✓		✓✓		✓			✓		✓			
Forensic Computing	University of Portsmouth	✓			✓												✓
Computer Science with Cyber Security with Professional Experience	The University of Salford	✓✓										✓					✓
Computer Security with Forensics	Sheffield Hallam University	✓			✓						✓	✓		✓			
Computer Forensics	University of South Wales	✓			✓			✓	✓✓				✓	✓			
Forensic Computing	Staffordshire University		✓			✓		✓	✓								
Computer Forensics	University of Sunderland	✓	✓		✓			✓	✓	✓		✓					
Computer and Digital Forensics	Teesside University		✓	✓				✓✓					✓✓			✓	

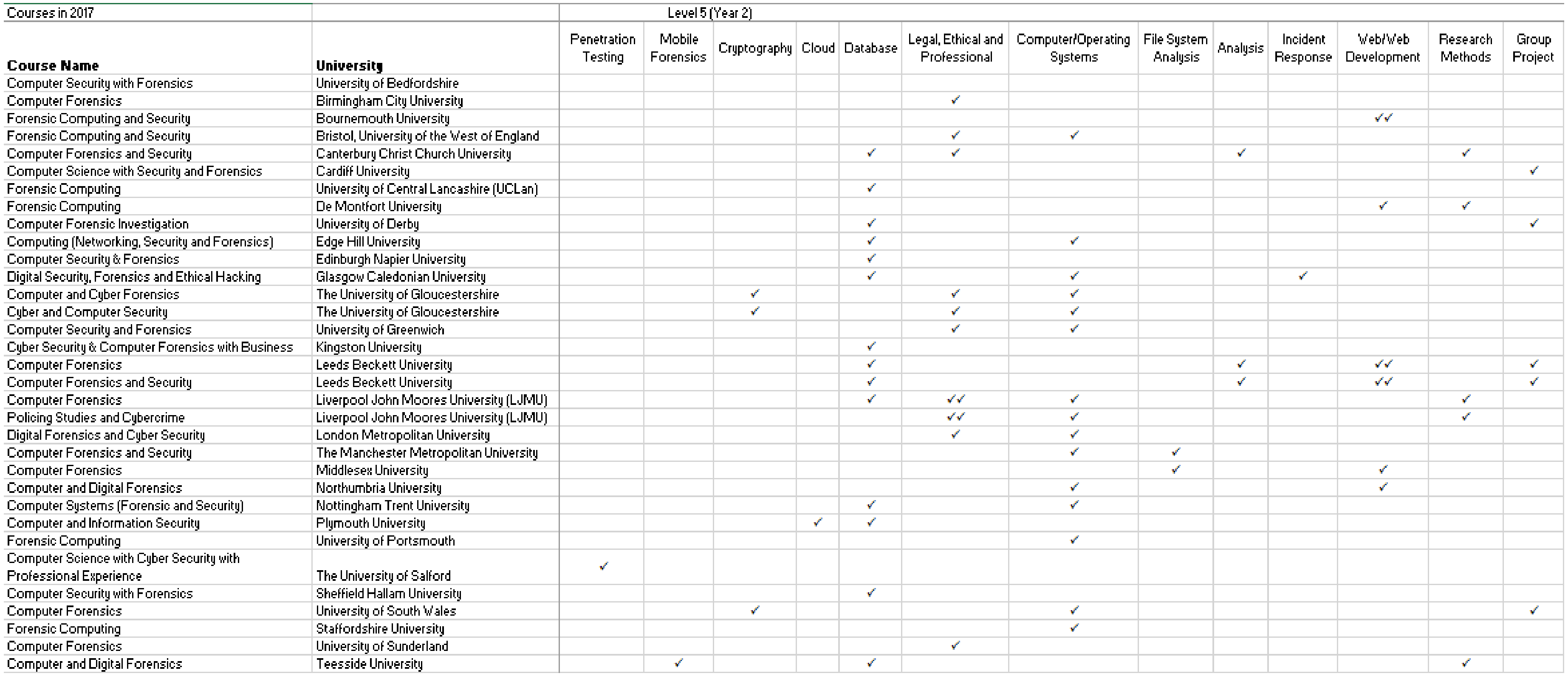
Figure C.2.1 Course offerings by themed topic and level 4 study

C.3 Level 5 Course Offerings by Topics

Courses in 2017										
Course Name	**University**	Programming	Software Development	Scripting	Networking	Network Forensics/ Investigation	Digital/Computer Forensics	Security/Computer Security	Ethical Hacking	Mobile Application/ Development/ Communications
Computer Security with Forensics	University of Bedfordshire				✓✓		✓	✓		
Computer Forensics	Birmingham City University	✓			✓		✓			
Forensic Computing and Security	Bournemouth University	✓✓					✓	✓	✓	
Forensic Computing and Security	Bristol, University of the West of England						✓	✓		
Computer Forensics and Security	Canterbury Christ Church University			✓	✓		✓	✓		
Computer Science with Security and Forensics	Cardiff University				✓					
Forensic Computing	University of Central Lancashire (UCLan)	✓			✓		✓	✓		
Forensic Computing	De Montfort University						✓	✓		
Computer Forensic Investigation	University of Derby				✓	✓	✓	✓		
Computing (Networking, Security and Forensics)	Edge Hill University				✓✓		✓	✓		✓
Computer Security & Forensics	Edinburgh Napier University				✓		✓			
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University				✓✓		✓	✓		
Computer and Cyber Forensics	The University of Gloucestershire						✓✓	✓✓	✓	
Cyber and Computer Security	The University of Gloucestershire							✓✓✓✓	✓	
Computer Security and Forensics	University of Greenwich				✓✓		✓	✓		
Cyber Security & Computer Forensics with Business	Kingston University				✓		✓		✓	
Computer Forensics	Leeds Beckett University				✓✓		✓✓	✓✓		
Computer Forensics and Security	Leeds Beckett University						✓✓	✓✓		
Computer Forensics	Liverpool John Moores University (LJMU)						✓			
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)						✓			
Digital Forensics and Cyber Security	London Metropolitan University				✓		✓	✓✓		
Computer Forensics and Security	The Manchester Metropolitan University	✓			✓		✓			
Computer Forensics	Middlesex University						✓			
Computer and Digital Forensics	Northumbria University	✓✓			✓		✓	✓✓		
Computer Systems (Forensic and Security)	Nottingham Trent University				✓✓			✓		
Computer and Information Security	Plymouth University	✓✓						✓		
Forensic Computing	University of Portsmouth				✓✓		✓✓	✓		
Computer Science with Cyber Security with Professional Experience	The University of Salford				✓✓			✓		
Computer Security with Forensics	Sheffield Hallam University				✓✓✓		✓	✓		
Computer Forensics	University of South Wales						✓	✓		
Forensic Computing	Staffordshire University	✓✓					✓✓	✓	✓	
Computer Forensics	University of Sunderland				✓		✓✓		✓	
Computer and Digital Forensics	Teesside University		✓	✓			✓			

Figure C.3.2 Course offerings by themed topics and level 5 study

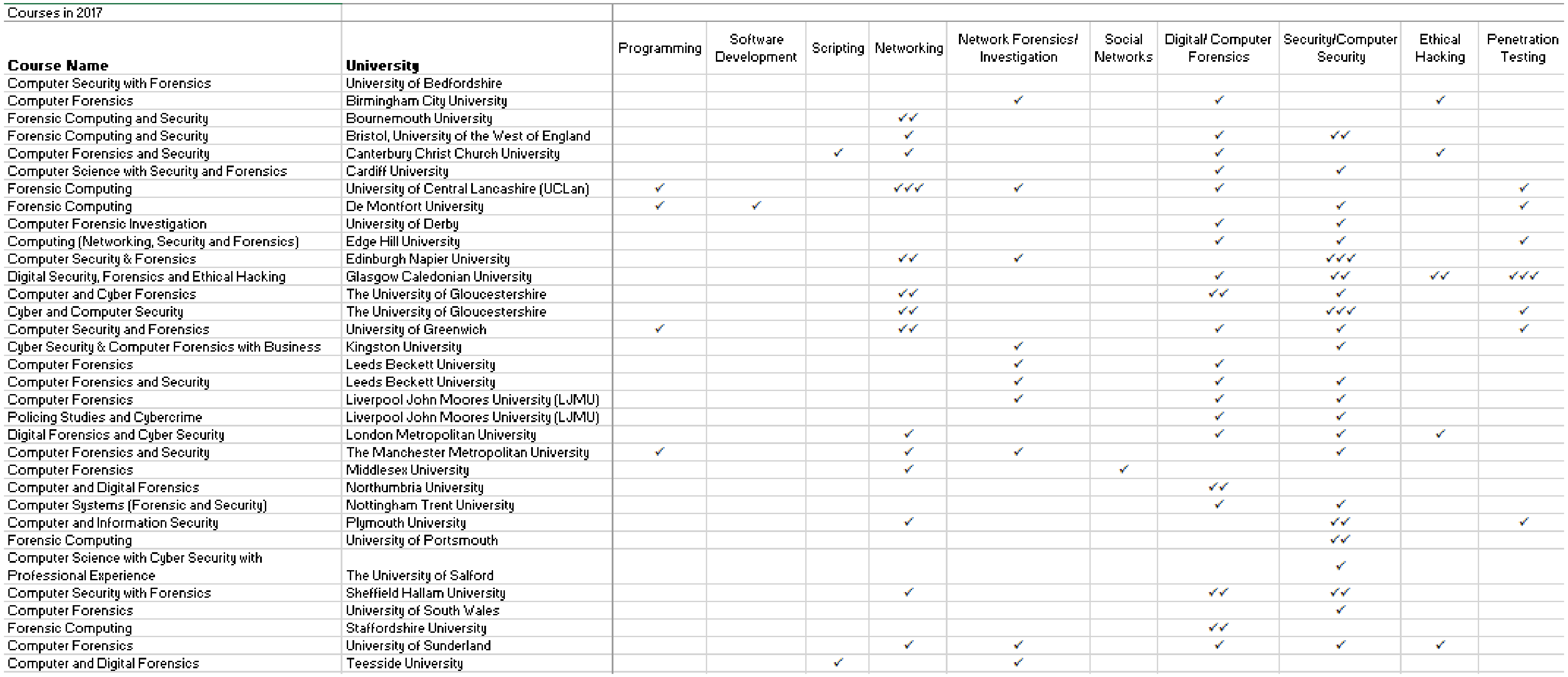
Continued on the next page



Courses in 2017		Level 5 (Year 2)												
Course Name	**University**	Penetration Testing	Mobile Forensics	Cryptography	Cloud	Database	Legal, Ethical and Professional	Computer/Operating Systems	File System Analysis	Analysis	Incident Response	Web/Web Development	Research Methods	Group Project
Computer Security with Forensics	University of Bedfordshire													
Computer Forensics	Birmingham City University						✓							
Forensic Computing and Security	Bournemouth University											✓✓		
Forensic Computing and Security	Bristol, University of the West of England						✓	✓						
Computer Forensics and Security	Canterbury Christ Church University					✓	✓			✓			✓	
Computer Science with Security and Forensics	Cardiff University													✓
Forensic Computing	University of Central Lancashire (UCLan)					✓								
Forensic Computing	De Montfort University											✓	✓	
Computer Forensic Investigation	University of Derby					✓								✓
Computing (Networking, Security and Forensics)	Edge Hill University					✓		✓						
Computer Security & Forensics	Edinburgh Napier University					✓								
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University					✓		✓			✓			
Computer and Cyber Forensics	The University of Gloucestershire			✓			✓	✓						
Cyber and Computer Security	The University of Gloucestershire			✓			✓	✓						
Computer Security and Forensics	University of Greenwich						✓	✓						
Cyber Security & Computer Forensics with Business	Kingston University					✓								
Computer Forensics	Leeds Beckett University					✓				✓		✓✓		✓
Computer Forensics and Security	Leeds Beckett University					✓				✓		✓✓		✓
Computer Forensics	Liverpool John Moores University (LJMU)					✓	✓✓	✓					✓	
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)						✓✓	✓					✓	
Digital Forensics and Cyber Security	London Metropolitan University						✓	✓						
Computer Forensics and Security	The Manchester Metropolitan University							✓	✓					
Computer Forensics	Middlesex University								✓			✓		
Computer and Digital Forensics	Northumbria University							✓				✓		
Computer Systems (Forensic and Security)	Nottingham Trent University					✓		✓						
Computer and Information Security	Plymouth University				✓	✓								
Forensic Computing	University of Portsmouth							✓						
Computer Science with Cyber Security with Professional Experience	The University of Salford	✓												
Computer Security with Forensics	Sheffield Hallam University					✓								
Computer Forensics	University of South Wales			✓				✓						✓
Forensic Computing	Staffordshire University							✓						
Computer Forensics	University of Sunderland						✓							
Computer and Digital Forensics	Teesside University		✓			✓							✓	

Figure C.3.3 Course offerings by themed topics and level 5 study

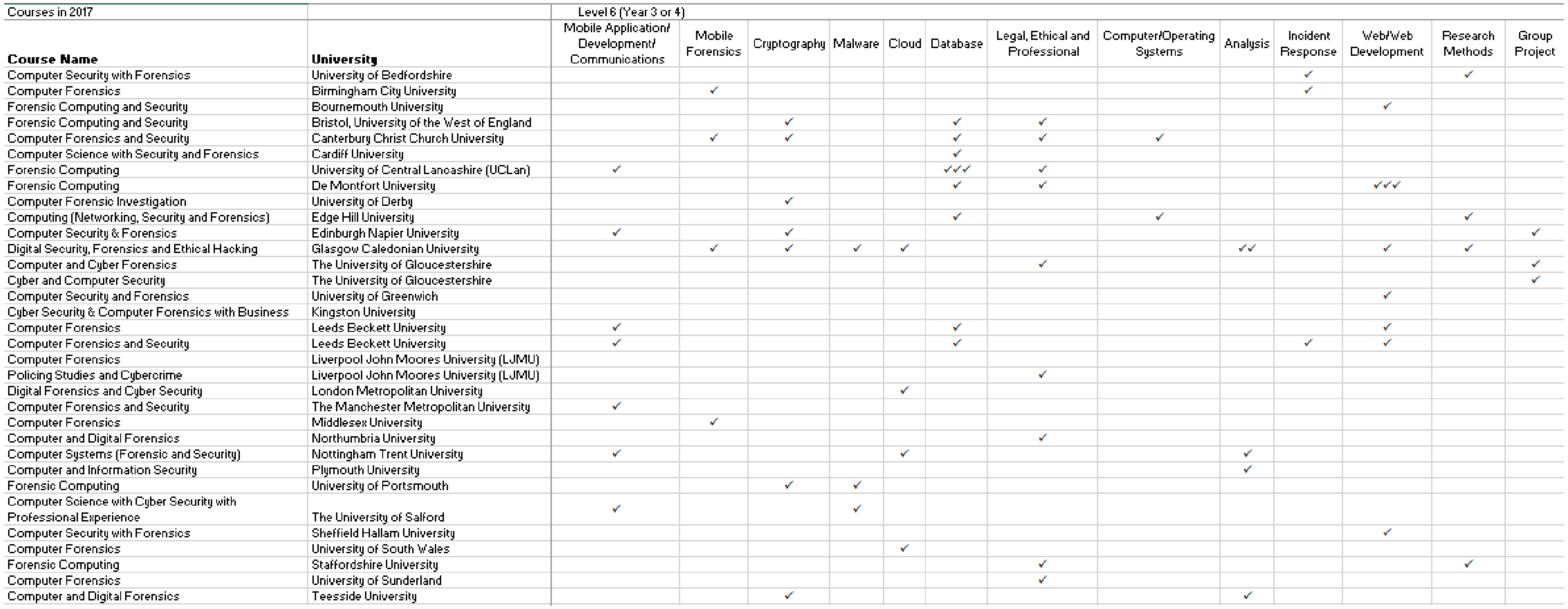
C.4 Level 6 Course Offerings by Topics



Courses in 2017											
Course Name	**University**	Programming	Software Development	Scripting	Networking	Network Forensics/ Investigation	Social Networks	Digital/ Computer Forensics	Security/Computer Security	Ethical Hacking	Penetration Testing
Computer Security with Forensics	University of Bedfordshire										
Computer Forensics	Birmingham City University					✓		✓		✓	
Forensic Computing and Security	Bournemouth University				✓✓						
Forensic Computing and Security	Bristol, University of the West of England				✓			✓	✓✓		
Computer Forensics and Security	Canterbury Christ Church University			✓	✓			✓		✓	
Computer Science with Security and Forensics	Cardiff University							✓	✓		
Forensic Computing	University of Central Lancashire (UCLan)	✓			✓✓✓	✓		✓			✓
Forensic Computing	De Montfort University	✓	✓						✓		✓
Computer Forensic Investigation	University of Derby							✓	✓		
Computing (Networking, Security and Forensics)	Edge Hill University							✓	✓		✓
Computer Security & Forensics	Edinburgh Napier University				✓✓	✓			✓✓✓		
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University							✓	✓✓	✓✓	✓✓✓
Computer and Cyber Forensics	The University of Gloucestershire				✓✓			✓✓	✓		
Cyber and Computer Security	The University of Gloucestershire				✓✓				✓✓✓		✓
Computer Security and Forensics	University of Greenwich	✓			✓✓			✓	✓		✓
Cyber Security & Computer Forensics with Business	Kingston University					✓			✓		
Computer Forensics	Leeds Beckett University					✓		✓			
Computer Forensics and Security	Leeds Beckett University					✓		✓	✓		
Computer Forensics	Liverpool John Moores University (LJMU)					✓		✓	✓		
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)							✓	✓		
Digital Forensics and Cyber Security	London Metropolitan University				✓			✓	✓	✓	
Computer Forensics and Security	The Manchester Metropolitan University	✓			✓	✓			✓		
Computer Forensics	Middlesex University				✓		✓				
Computer and Digital Forensics	Northumbria University							✓✓			
Computer Systems (Forensic and Security)	Nottingham Trent University							✓	✓		
Computer and Information Security	Plymouth University				✓				✓✓		✓
Forensic Computing	University of Portsmouth								✓✓		
Computer Science with Cyber Security with Professional Experience	The University of Salford								✓		
Computer Security with Forensics	Sheffield Hallam University				✓			✓✓	✓✓		
Computer Forensics	University of South Wales								✓		
Forensic Computing	Staffordshire University							✓✓			
Computer Forensics	University of Sunderland				✓	✓		✓	✓	✓	
Computer and Digital Forensics	Teesside University			✓		✓					

Figure C.4.4 Course offerings by themed topics and level 6 study

Continued on the next page



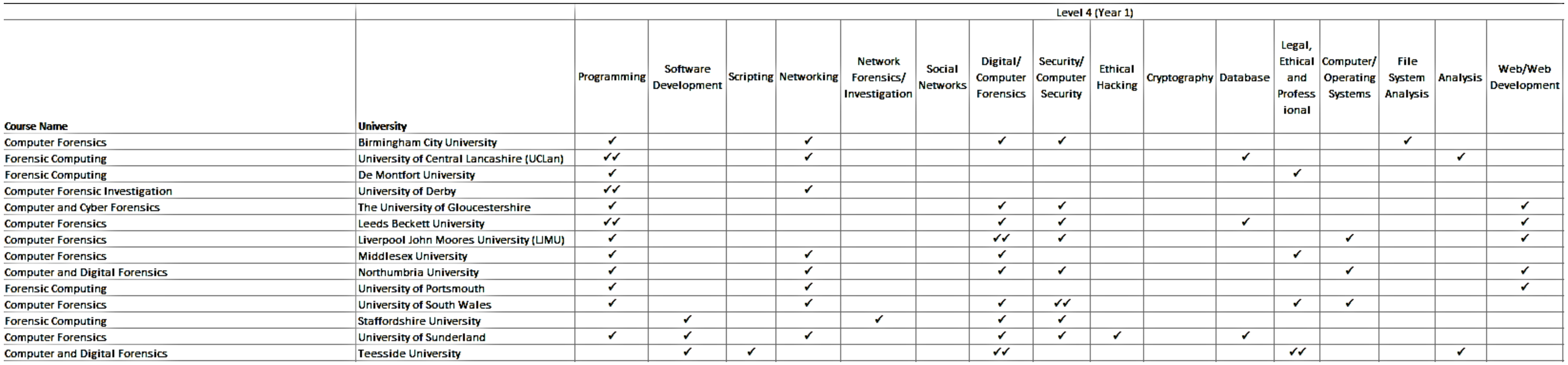
Courses in 2017		Level 6 (Year 3 or 4)												
Course Name	**University**	Mobile Application/ Development/ Communications	Mobile Forensics	Cryptography	Malware	Cloud	Database	Legal, Ethical and Professional	Computer/Operating Systems	Analysis	Incident Response	Web/Web Development	Research Methods	Group Project
Computer Security with Forensics	University of Bedfordshire										✓		✓	
Computer Forensics	Birmingham City University		✓								✓			
Forensic Computing and Security	Bournemouth University											✓		
Forensic Computing and Security	Bristol, University of the West of England			✓			✓	✓						
Computer Forensics and Security	Canterbury Christ Church University		✓	✓			✓	✓	✓					
Computer Science with Security and Forensics	Cardiff University						✓							
Forensic Computing	University of Central Lancashire (UCLan)	✓					✓✓✓	✓						
Forensic Computing	De Montfort University						✓	✓				✓✓✓		
Computer Forensic Investigation	University of Derby			✓										
Computing (Networking, Security and Forensics)	Edge Hill University						✓		✓				✓	
Computer Security & Forensics	Edinburgh Napier University	✓		✓										✓
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University		✓	✓	✓	✓				✓✓		✓	✓	
Computer and Cyber Forensics	The University of Gloucestershire							✓						✓
Cyber and Computer Security	The University of Gloucestershire													✓
Computer Security and Forensics	University of Greenwich											✓		
Cyber Security & Computer Forensics with Business	Kingston University													
Computer Forensics	Leeds Beckett University	✓					✓					✓		
Computer Forensics and Security	Leeds Beckett University	✓					✓				✓	✓		
Computer Forensics	Liverpool John Moores University (LJMU)													
Policing Studies and Cybercrime	Liverpool John Moores University (LJMU)							✓						
Digital Forensics and Cyber Security	London Metropolitan University					✓								
Computer Forensics and Security	The Manchester Metropolitan University	✓												
Computer Forensics	Middlesex University		✓											
Computer and Digital Forensics	Northumbria University							✓						
Computer Systems (Forensic and Security)	Nottingham Trent University	✓				✓				✓				
Computer and Information Security	Plymouth University									✓				
Forensic Computing	University of Portsmouth			✓	✓									
Computer Science with Cyber Security with Professional Experience	The University of Salford	✓			✓									
Computer Security with Forensics	Sheffield Hallam University											✓		
Computer Forensics	University of South Wales					✓								
Forensic Computing	Staffordshire University							✓					✓	
Computer Forensics	University of Sunderland							✓						
Computer and Digital Forensics	Teesside University			✓						✓				

Figure C.4.5 Course offerings by themed topics and level 6 study

C.5 Course Offerings by Digital Forensic Courses

The following tables demonstrate each course categorised as belonging more to the digital/computer forensics categorisation by course naming convention (e.g. cyber security is not included in the title). Each figure demonstrates common module topics included within such a course.

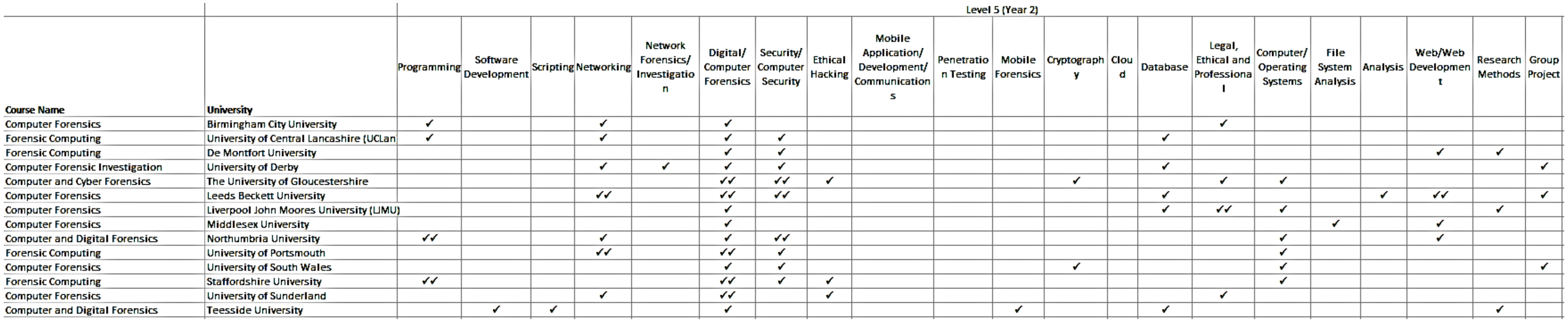
C.5.1 Level 4



		Level 4 (Year 1)																
Course Name	**University**	Programming	Software Development	Scripting	Networking	Network Forensics/ Investigation	Social Networks	Digital/ Computer Forensics	Security/ Computer Security	Ethical Hacking	Cryptography	Database	Legal, Ethical and Professional	Computer/ Operating Systems	File System Analysis	Analysis	Web/Web Development
Computer Forensics	Birmingham City University	✓			✓			✓	✓						✓		
Forensic Computing	University of Central Lancashire (UCLan)	✓✓			✓							✓				✓	
Forensic Computing	De Montfort University	✓											✓				
Computer Forensic Investigation	University of Derby	✓✓			✓												
Computer and Cyber Forensics	The University of Gloucestershire	✓						✓	✓								✓
Computer Forensics	Leeds Beckett University	✓✓						✓	✓			✓					✓
Computer Forensics	Liverpool John Moores University (LJMU)	✓						✓✓	✓					✓			✓
Computer Forensics	Middlesex University	✓			✓			✓					✓				
Computer and Digital Forensics	Northumbria University	✓			✓			✓	✓					✓			✓
Forensic Computing	University of Portsmouth	✓			✓												✓
Computer Forensics	University of South Wales	✓			✓			✓	✓✓				✓	✓			
Forensic Computing	Staffordshire University		✓			✓		✓	✓								
Computer Forensics	University of Sunderland	✓	✓		✓			✓	✓	✓		✓					
Computer and Digital Forensics	Teesside University		✓	✓				✓✓					✓✓			✓	

Figure C.5.1.1 Course offerings for digital forensics by themed topics and level 4 study

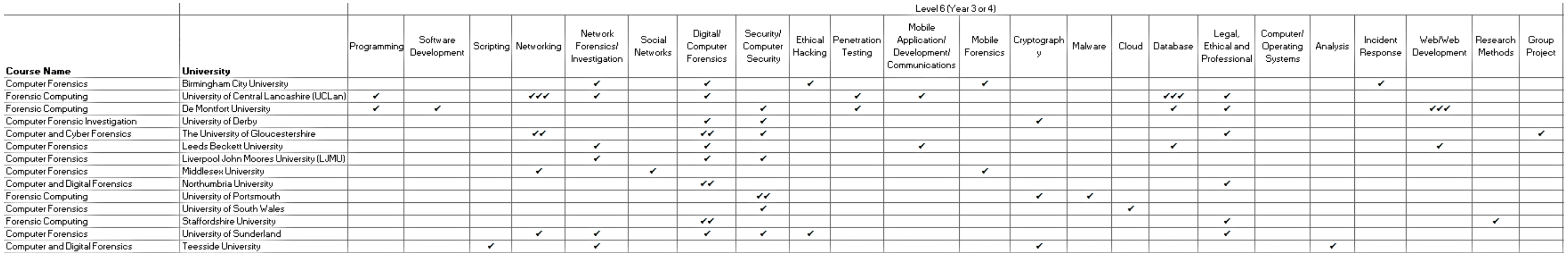
C.5.2 Level 5



		Level 5 (Year 2)																				
Course Name	**University**	Programming	Software Development	Scripting	Networking	Network Forensics/ Investigation	Digital/ Computer Forensics	Security/ Computer Security	Ethical Hacking	Mobile Application/ Development/ Communications	Penetration Testing	Mobile Forensics	Cryptography	Cloud	Database	Legal, Ethical and Professional	Computer/ Operating Systems	File System Analysis	Analysis	Web/Web Development	Research Methods	Group Project
Computer Forensics	Birmingham City University	✓			✓		✓									✓						
Forensic Computing	University of Central Lancashire (UCLan	✓			✓		✓	✓							✓							
Forensic Computing	De Montfort University						✓	✓												✓	✓	
Computer Forensic Investigation	University of Derby				✓	✓	✓	✓							✓							✓
Computer and Cyber Forensics	The University of Gloucestershire						✓✓	✓✓	✓				✓			✓	✓					
Computer Forensics	Leeds Beckett University				✓✓		✓✓	✓✓							✓				✓	✓✓		✓
Computer Forensics	Liverpool John Moores University (LJMU)						✓								✓	✓✓	✓				✓	
Computer Forensics	Middlesex University						✓											✓		✓		
Computer and Digital Forensics	Northumbria University	✓✓			✓		✓	✓✓									✓			✓		
Forensic Computing	University of Portsmouth				✓✓		✓✓	✓									✓					
Computer Forensics	University of South Wales						✓	✓					✓				✓					✓
Forensic Computing	Staffordshire University	✓✓					✓✓	✓	✓								✓					
Computer Forensics	University of Sunderland				✓		✓✓		✓							✓						
Computer and Digital Forensics	Teesside University		✓	✓			✓					✓			✓						✓	

Figure C.5.2.2 Course offerings for digital forensics by themed topics and level 5 study

C.5.3 Level 6



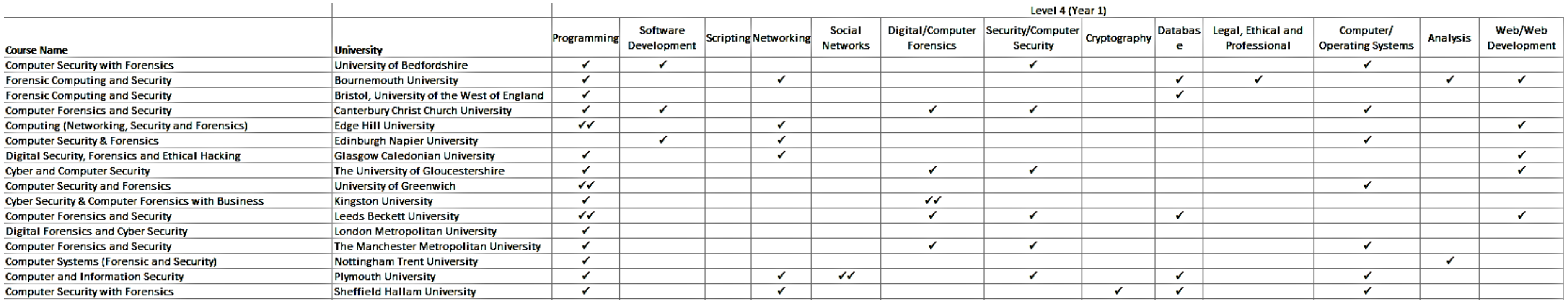
		Level 6 (Year 3 or 4)																						
Course Name	**University**	Programming	Software Development	Scripting	Networking	Network Forensics/ Investigation	Social Networks	Digital/ Computer Forensics	Security/ Computer Security	Ethical Hacking	Penetration Testing	Mobile Application/ Development/ Communications	Mobile Forensics	Cryptograph y	Malware	Cloud	Database	Legal, Ethical and Professional	Computer/ Operating Systems	Analysis	Incident Response	Web/Web Development	Research Methods	Group Project
Computer Forensics	Birmingham City University					✓		✓		✓			✓								✓			
Forensic Computing	University of Central Lancashire (UCLan)	✓			✓✓✓	✓		✓			✓	✓					✓✓✓	✓						
Forensic Computing	De Montfort University	✓	✓						✓		✓						✓	✓				✓✓✓		
Computer Forensic Investigation	University of Derby							✓	✓					✓										
Computer and Cyber Forensics	The University of Gloucestershire				✓✓			✓✓	✓									✓						✓
Computer Forensics	Leeds Beckett University					✓		✓				✓					✓					✓		
Computer Forensics	Liverpool John Moores University (LJMU)					✓		✓	✓															
Computer Forensics	Middlesex University				✓		✓						✓											
Computer and Digital Forensics	Northumbria University							✓✓										✓						
Forensic Computing	University of Portsmouth								✓✓					✓	✓									
Computer Forensics	University of South Wales								✓							✓								
Forensic Computing	Staffordshire University							✓✓										✓					✓	
Computer Forensics	University of Sunderland				✓	✓		✓	✓	✓								✓						
Computer and Digital Forensics	Teesside University			✓		✓								✓						✓				

Figure C.5.3.3 Course offerings for digital forensics by themed topics and level 5 study

C.6 Course Offerings by Digital Forensic and Security Courses

The following tables demonstrate courses categorised as belonging more to the both disciplines (e.g. forensics and security are included in the course title). Each figure demonstrates common module topics included within such a course.

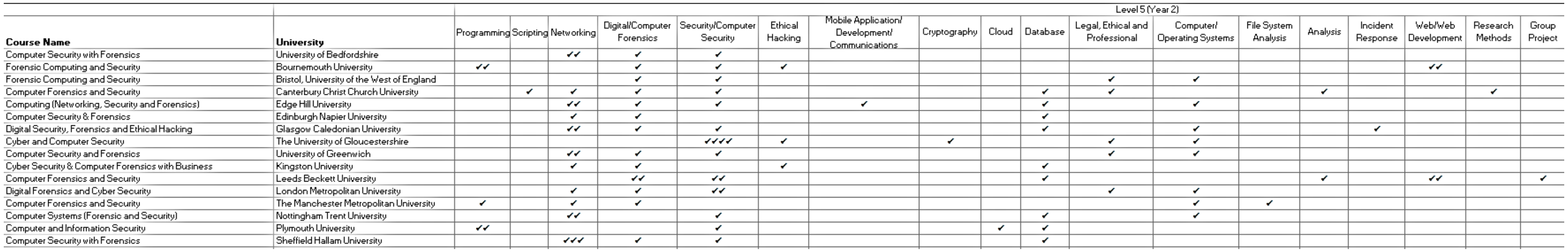
C.6.1 Level 4



		Level 4 (Year 1)												
Course Name	University	Programming	Software Development	Scripting	Networking	Social Networks	Digital/Computer Forensics	Security/Computer Security	Cryptography	Databas e	Legal, Ethical and Professional	Computer/ Operating Systems	Analysis	Web/Web Development
Computer Security with Forensics	University of Bedfordshire	✓	✓					✓				✓		
Forensic Computing and Security	Bournemouth University	✓			✓					✓	✓		✓	✓
Forensic Computing and Security	Bristol, University of the West of England	✓								✓				
Computer Forensics and Security	Canterbury Christ Church University	✓	✓				✓	✓				✓		
Computing (Networking, Security and Forensics)	Edge Hill University	✓✓			✓									✓
Computer Security & Forensics	Edinburgh Napier University		✓		✓							✓		
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University	✓			✓									✓
Cyber and Computer Security	The University of Gloucestershire	✓					✓	✓						✓
Computer Security and Forensics	University of Greenwich	✓✓										✓		
Cyber Security & Computer Forensics with Business	Kingston University	✓					✓✓							
Computer Forensics and Security	Leeds Beckett University	✓✓					✓	✓		✓				✓
Digital Forensics and Cyber Security	London Metropolitan University	✓												
Computer Forensics and Security	The Manchester Metropolitan University	✓					✓	✓				✓		
Computer Systems (Forensic and Security)	Nottingham Trent University	✓											✓	
Computer and Information Security	Plymouth University	✓			✓	✓✓		✓		✓		✓		
Computer Security with Forensics	Sheffield Hallam University	✓			✓				✓	✓		✓		

Figure C.6.1.1 Course offerings for digital forensics and security by themed topics and level 4 study

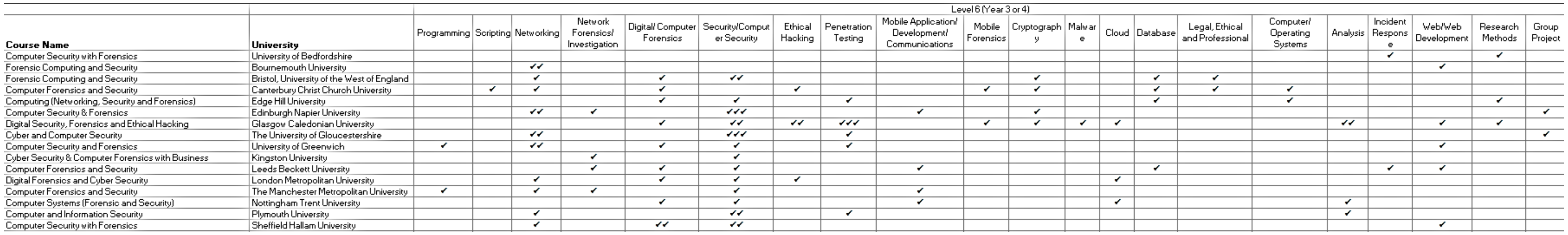
C.6.2 Level 5



		Level 5 (Year 2)																	
Course Name	University	Programming	Scripting	Networking	Digital/Computer Forensics	Security/Computer Security	Ethical Hacking	Mobile Application/ Development/ Communications	Cryptography	Cloud	Database	Legal, Ethical and Professional	Computer/ Operating Systems	File System Analysis	Analysis	Incident Response	Web/Web Development	Research Methods	Group Project
Computer Security with Forensics	University of Bedfordshire			✓✓	✓	✓													
Forensic Computing and Security	Bournemouth University	✓✓			✓	✓	✓										✓✓		
Forensic Computing and Security	Bristol, University of the West of England				✓	✓						✓	✓						
Computer Forensics and Security	Canterbury Christ Church University		✓	✓	✓	✓					✓	✓			✓			✓	
Computing (Networking, Security and Forensics)	Edge Hill University			✓✓	✓	✓		✓			✓		✓						
Computer Security & Forensics	Edinburgh Napier University			✓	✓						✓								
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University			✓✓	✓	✓					✓		✓			✓			
Cyber and Computer Security	The University of Gloucestershire					✓✓✓✓	✓		✓			✓	✓						
Computer Security and Forensics	University of Greenwich			✓✓	✓	✓						✓	✓						
Cyber Security & Computer Forensics with Business	Kingston University			✓	✓		✓				✓								
Computer Forensics and Security	Leeds Beckett University				✓✓	✓✓					✓				✓		✓✓		✓
Digital Forensics and Cyber Security	London Metropolitan University			✓	✓	✓✓						✓	✓						
Computer Forensics and Security	The Manchester Metropolitan University	✓		✓	✓								✓	✓					
Computer Systems (Forensic and Security)	Nottingham Trent University			✓✓		✓					✓		✓						
Computer and Information Security	Plymouth University	✓✓				✓				✓	✓								
Computer Security with Forensics	Sheffield Hallam University			✓✓✓	✓	✓					✓								

Figure C.6.2.2 Course offerings for digital forensics and security by themed topics and level 5 study

C.6.3 Level 6



		Level 6 (Year 3 or 4)																				
Course Name	**University**	Programming	Scripting	Networking	Network Forensics/ Investigation	Digital/ Computer Forensics	Security/Computer Security	Ethical Hacking	Penetration Testing	Mobile Application/ Development/ Communications	Mobile Forensics	Cryptography	Malware	Cloud	Database	Legal, Ethical and Professional	Computer/ Operating Systems	Analysis	Incident Response	Web/Web Development	Research Methods	Group Project
Computer Security with Forensics	University of Bedfordshire																		✓		✓	
Forensic Computing and Security	Bournemouth University			✓✓																✓		
Forensic Computing and Security	Bristol, University of the West of England			✓		✓	✓✓					✓			✓	✓						
Computer Forensics and Security	Canterbury Christ Church University		✓	✓		✓		✓			✓	✓			✓	✓	✓					
Computing (Networking, Security and Forensics)	Edge Hill University					✓	✓		✓						✓		✓				✓	
Computer Security & Forensics	Edinburgh Napier University			✓✓	✓		✓✓✓			✓		✓										✓
Digital Security, Forensics and Ethical Hacking	Glasgow Caledonian University					✓	✓✓	✓✓	✓✓✓		✓	✓	✓	✓				✓✓		✓	✓	
Cyber and Computer Security	The University of Gloucestershire			✓✓			✓✓✓		✓													✓
Computer Security and Forensics	University of Greenwich	✓		✓✓		✓	✓		✓											✓		
Cyber Security & Computer Forensics with Business	Kingston University				✓		✓															
Computer Forensics and Security	Leeds Beckett University				✓	✓	✓			✓					✓				✓	✓		
Digital Forensics and Cyber Security	London Metropolitan University			✓		✓	✓	✓						✓								
Computer Forensics and Security	The Manchester Metropolitan University	✓		✓	✓		✓			✓												
Computer Systems (Forensic and Security)	Nottingham Trent University					✓	✓			✓				✓				✓				
Computer and Information Security	Plymouth University			✓			✓✓		✓									✓				
Computer Security with Forensics	Sheffield Hallam University			✓		✓✓	✓✓													✓		

Figure C.6.3.3 Course offerings for digital forensics and security by themed topics and level 6 study

C.7 Computer Science courses with a flavour in HE

While conducting the search for courses relating to digital forensics and cyber security, computer science courses were not considered too closely, unless forensics and security were included in the programme title. However, these courses should be mentioned.

Using data previously obtained from UCAS and HESA courses directed at computer science with a flavour of security, be it information or cyber security, have existed since before 2011. The data shows that these courses have often emerged at master's level, throughout 2011 to the time of writing. Examples of security flavoured undergraduate courses which existed before 2011 include Computer Science (Information Security) at the Royal Holloway University and Staffordshire University; Forensic Science with Computer Science at Keele University and De Montfort University. In 2012 Newcastle University added a course in Computer Science (Security and Resilience) while other offerings included master's level studies in computer science with security or dedicated cyber security master's programmes. These were just a few instances where courses had been offered.

While the main aim of this thesis is to focus on courses based around digital forensics and cyber security those of a computer science grounding with a flavour of security are briefly considered below. Three courses were looked at; one chosen due to the length of time it has been on offer at The Royal Holloway University and its incorporated masters. Another chosen due to its later development at Newcastle University, and another for its year for 'professional experience' at The University of Salford.

From these courses, The Royal Holloway University provided the most flexibility in the number of optional modules available (four modules at level 5; nineteen modules at level 6 and 18 modules at MSci). It could be argued this flexibility allows students to diversify their learning into new domains and strengthen their unique position in terms of employability. Newcastle University was next to offer a range of optional modules with a total of 18. The University of Salford provided less optional modules but included a professional experience year where the course flavour focused on cyber security.

A quick analysis of these three courses showed that common modules and often core to the course delivery were programming and software engineering. 'Programming' and 'Software' were both mentioned on ten occasions including examples such as, understanding programming languages, concurrent and parallel programming, software engineering, software verifications technologies and malicious software. Mathematics and algorithms were included in all three courses (7 occasions), where at least one module exists on each course. 'System' was mentioned on 15 occasions including Embedded, Real-Time, Mobile, Operating, Distributed and Intelligent systems in naming convention. Databases were mentioned once at each institution.

When looking to elements of flavour of security, the keyword 'security' was mentioned on 8 occasions across the three courses. 4 of these modules included networking in the title and others were based on introductory elements of security, management and testing. Networking was mentioned on six occasions in total across these courses. 'Cyber' was mentioned on one occasion at each course, a total of three modules focusing on systems and security. 'Information Security' was mentioned once by two of the institutions in module naming convention. These low number of occurrences are interesting given the flavour of the courses; however, it is not astonishing due to the main focus being computer science.

Web was mentioned on five occasions across the three courses covering aspects of web design, construction, management and technologies. Looking to more unique module offerings, gaming was mentioned in all three courses, on seven occasions, in the form of examples such as Virtual Reality and 3D Games, Games Labs, Graphics for Games and Computer games technologies. AI was mentioned in two courses; Robotics in one course offering and Malware also in one course module. While other offerings concentrated on systems, software and applications and programming.

'Digital Forensics' was mentioned on one course at master's level as an optional module. Highlighting again that the focus for many has shifted toward cyber and information security. Although, it should be noted that the majority of naming conventions for these modules strongly pertain to the fundamentals of computer science and security is once more a flavouring.

APPENDIX D – STUDENT WORKSHOP STATISTICAL ANALYSIS

This appendix provides results of statistical tests conducted in chapter 8.

D.1 Identifying nonresponses

Students were asked to consider several topics/skills which are related, in particularly, to digital forensics curriculum as well as several which relate to cyber security. In the tables below all responses are grouped and nonresponses are identified by each item. In total there were 11 nonresponses across the 27 items provided to students. All eleven were found in one workshop/group.

		Fundamentals of Computing	Basic Forensic Procedures	Legal, Professional and Ethical Issues	Policing and Criminal Justice	Court Room Skills	Mobile Forensics	Linux Forensics	Mac Forensics	Live Data Forensics
N	Valid	39	39	39	38	38	38	38	38	38
	Missing	0	0	0	1	1	1	1	1	1

		Digital Forensics Tools (Proprietary)	Digital Forensics Tools (Open Source)	Linux as an Investigative Tool	Software Engineering/ Development	Scripting/ Programming	Pen Testing Techniques and Tools	Ethical Hacking and Countermeasures
N	Valid	38	38	38	39	39	39	39
	Missing	1	1	1	0	0	0	0

		Information Security and Assurance	Server Infrastructure	Networks	Databases	Operating, File and Computer Systems	Cryptography	Computational Mathematics	Internet of Things
N	Valid	39	39	39	39	39	39	38	39
	Missing	0	0	0	0	0	0	1	0

		Contemporary Issues/Emerging Technologies	Employability Skills	Project Management
N	Valid	38	39	39
	Missing	1	0	0

D.2 Descriptive Statistics – SPSS

This section includes all descriptive statistics conducted to examine the topics students felt, of those they were provided with, were important. There are three tables, one per group and one for all students combined.

Descriptive Statistics

What subjects do you think a degree in digital forensics and cyber security should include?	N	Range	Min	Max	Sum	Mean	Std. Deviation
Fundamentals of Computing	39	4	1	5	158	4.05	.999
Basic Forensic Procedures	39	2	3	5	179	4.59	.637
Legal, Professional and Ethical Issues	39	3	2	5	164	4.21	.894
Policing and Criminal Justice	39	5	0	5	141	3.62	1.161
Court Room Skills	39	5	0	5	136	3.49	1.144
Mobile Forensics	39	5	0	5	169	4.33	1.060
Linux Forensics	39	5	0	5	162	4.15	1.065
Mac Forensics	39	5	0	5	154	3.95	1.099
Live Data Forensics	39	5	0	5	167	4.28	.972
Digital Forensics Tools (Proprietary)	39	5	0	5	171	4.38	1.138
Digital Forensics Tools (Open Source)	39	5	0	5	172	4.41	.993
Linux as an Investigative Tool	39	5	0	5	158	4.05	.999
Software Engineering/Development	39	4	1	5	123	3.15	1.065
Scripting/Programming	39	3	2	5	151	3.87	1.005
Pen Testing Techniques and Tools	39	3	2	5	167	4.28	.826
Ethical Hacking and Countermeasures	39	2	3	5	178	4.56	.641
Information Security and Assurance	39	2	3	5	171	4.38	.633
Server Infrastructure	39	3	2	5	148	3.79	.978
Networks	39	3	2	5	169	4.33	.838
Databases	39	3	2	5	146	3.74	.966
Operating, File and Computer Systems	39	3	2	5	162	4.15	.933
Cryptography	39	3	2	5	164	4.21	.923
Computational Mathematics	39	5	0	5	128	3.28	1.146
Internet of Things	39	3	2	5	156	4.00	.889
Contemporary Issues/Emerging Technologies	39	5	0	5	152	3.90	1.142
Employability Skills	39	4	1	5	157	4.03	1.135
Project Management	39	4	1	5	136	3.49	1.393
Valid N (listwise)	39						

Descriptive Statistics [a]

What subjects do you think a degree in digital forensics and cyber security should include?	N	Min	Max	Mean	Std. Deviation	Skewness		Kurtosis	
		Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Basic Forensic Procedures	16	4	5	4.56	.512	-.279	.564	-2.219	1.091
Information Security and Assurance	16	3	5	4.56	.629	-1.183	.564	.633	1.091
Ethical Hacking and Countermeasures	16	4	5	4.56	.512	-.279	.564	-2.219	1.091
Pen Testing Techniques and Tools	16	4	5	4.56	.512	-.279	.564	-2.219	1.091
Digital Forensics Tools (Open Source)	16	3	5	4.56	.629	-1.183	.564	.633	1.091
Live Data Forensics	16	3	5	4.50	.632	-.904	.564	.027	1.091
Digital Forensics Tools (Proprietary)	16	1	5	4.44	1.031	-2.731	.564	8.719	1.091
Linux Forensics	16	2	5	4.38	.885	-1.545	.564	2.277	1.091
Mobile Forensics	16	2	5	4.38	.885	-1.545	.564	2.277	1.091
Linux as an Investigative Tool	16	3	5	4.31	.793	-.662	.564	-1.006	1.091
Networks	16	2	5	4.25	.931	-1.133	.564	.677	1.091
Legal, Professional and Ethical Issues	16	3	5	4.25	.931	-.567	.564	-1.711	1.091
Mac Forensics	16	2	5	4.19	.911	-1.019	.564	.629	1.091
Operating, File and Computer Systems	16	2	5	3.94	1.124	-.507	.564	-1.196	1.091
Databases	16	2	5	3.88	1.258	-.423	.564	-1.633	1.091
Contemporary Issues/Emerging Technologies	16	2	5	3.81	1.047	-.375	.564	-.948	1.091
Scripting/Programming	16	2	5	3.81	.981	-.062	.564	-1.197	1.091
Cryptography	16	2	5	3.75	1.065	-.189	.564	-1.183	1.091
Policing and Criminal Justice	16	1	5	3.75	1.125	-.722	.564	.720	1.091
Employability Skills	16	1	5	3.69	1.302	-.782	.564	-.535	1.091
Court Room Skills	16	1	5	3.63	1.025	-.810	.564	1.645	1.091
Internet of Things	16	2	5	3.63	.957	.374	.564	-1.035	1.091
Server Infrastructure	16	2	5	3.56	1.094	-.007	.564	-1.228	1.091
Fundamentals of Computing	16	1	5	3.56	1.153	-.770	.564	.149	1.091
Computational Mathematics	16	2	5	2.94	1.063	.900	.564	-.259	1.091
Software Engineering/Development	16	1	5	2.88	1.204	.270	.564	-.342	1.091
Project Management	16	1	5	2.63	1.544	.229	.564	-1.602	1.091
Valid N (listwise)	16								

a. Group = 1 || Workshop A

Descriptive Statistics [b]

	N	Min	Max	Mean	Std. Deviation	Skewness		Kurtosis	
What subjects do you think a degree in digital forensics and cyber security should include?		Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Basic Forensic Procedures	23	3	5	4.61	.722	-1.605	.481	1.130	.935
Ethical Hacking and Countermeasures	23	3	5	4.57	.728	-1.409	.481	.586	.935
Digital Forensics Tools (Proprietary)	22	3	5	4.55	.800	-1.388	.491	.176	.953
Cryptography	23	3	5	4.52	.665	-1.100	.481	.194	.935
Digital Forensics Tools (Open Source)	22	3	5	4.50	.740	-1.163	.491	-.019	.953
Mobile Forensics	22	3	5	4.50	.740	-1.163	.491	-.019	.953
Networks	23	3	5	4.39	.783	-.851	.481	-.765	.935
Fundamentals of Computing	23	3	5	4.39	.722	-.773	.481	-.587	.935
Live Data Forensics	22	3	5	4.32	.716	-.569	.491	-.756	.953
Operating, File and Computer Systems	23	3	5	4.30	.765	-.601	.481	-.974	.935
Employability Skills	23	2	5	4.26	.964	-.912	.481	-.503	.935
Internet of Things	23	3	5	4.26	.752	-.485	.481	-1.001	.935
Information Security and Assurance	23	3	5	4.26	.619	-.212	.481	-.408	.935
Linux Forensics	22	3	5	4.18	.795	-.352	.491	-1.292	.953
Legal, Professional and Ethical Issues	23	2	5	4.17	.887	-.796	.481	-.117	.935
Contemporary Issues/Emerging Technologies	22	3	5	4.14	.889	-.287	.491	-1.730	.953
Project Management	23	2	5	4.09	.900	-.591	.481	-.527	.935
Pen Testing Techniques and Tools	23	2	5	4.09	.949	-.535	.481	-.934	.935
Linux as an Investigative Tool	22	3	5	4.05	.722	-.069	.491	-.929	.953
Server Infrastructure	23	2	5	3.96	.878	-.352	.481	-.644	.935
Mac Forensics	22	2	5	3.95	.899	-.338	.491	-.764	.953
Scripting/Programming	23	2	5	3.91	1.041	-.343	.481	-1.205	.935
Computational Mathematics	22	2	5	3.68	.894	-.167	.491	-.531	.953
Policing and Criminal Justice	22	2	5	3.68	.945	-.023	.491	-.871	.953
Databases	23	3	5	3.65	.714	.639	.481	-.695	.935
Court Room Skills	22	2	5	3.55	1.011	-.136	.491	-.955	.953
Software Engineering/Development	23	2	5	3.35	.935	.304	.481	-.577	.935
Valid N (listwise)	22								

b. Group = 2 || Workshop B

D.2.1 Frequency Statistics (per item - all students) – SPSS

Fundamentals of Computing

Fundamentals of Computing		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	15	38.5	38.5	38.5
	Important	15	38.5	38.5	76.9
	Moderately Important	6	15.4	15.4	92.3
	Slightly Important	2	5.1	5.1	97.4
	Not Important at all	1	2.6	2.6	100.0
	Total	39	100.0	100.0	

Basic Forensic Procedures

Basic Forensic Procedures		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	26	66.7	66.7	66.7
	Important	10	25.6	25.6	92.3
	Moderately Important	3	7.7	7.7	100.0
	Total	39	100.0	100.0	

Legal, Professional and Ethical Issues

Legal, Professional and Ethical Issues		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	19	48.7	48.7	48.7
	Important	10	25.6	25.6	74.4
	Moderately Important	9	23.1	23.1	97.4
	Slightly Important	1	2.6	2.6	100.0
	Total	39	100.0	100.0	

Policing and Criminal Justice

Policing and Criminal Justice		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	10	25.6	26.3	26.3
	Important	11	28.2	28.9	55.3
	Moderately Important	14	35.9	36.8	92.1
	Slightly Important	2	5.1	5.3	97.4
	Not Important at all	1	2.6	2.6	100.0
	Total	38	97.4	100.0	
Missing	No Opinion	1	2.6		
Total		39	100.0		

Court Room Skills

Court Room Skills		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	7	17.9	18.4	18.4
	Important	14	35.9	36.8	55.3
	Moderately Important	12	30.8	31.6	86.8
	Slightly Important	4	10.3	10.5	97.4
	Not Important at all	1	2.6	2.6	100.0
	Total	38	97.4	100.0	
Missing	No Opinion	1	2.6		
Total		39	100.0		

Mobile Forensics

Mobile Forensics		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	23	59.0	60.5	60.5
	Important	10	25.6	26.3	86.8
	Moderately Important	4	10.3	10.5	97.4
	Slightly Important	1	2.6	2.6	100.0
	Total	38	97.4	100.0	
Missing	No Opinion	1	2.6		
Total		39	100.0		

Linux Forensics

Linux Forensics		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	18	46.2	47.4	47.4
	Important	13	33.3	34.2	81.6
	Moderately Important	6	15.4	15.8	97.4
	Slightly Important	1	2.6	2.6	100.0
	Total	38	97.4	100.0	
Missing	No Opinion	1	2.6		
Total		39	100.0		

Mac Forensics

Mac Forensics		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	14	35.9	36.8	36.8
	Important	14	35.9	36.8	73.7
	Moderately Important	8	20.5	21.1	94.7
	Slightly Important	2	5.1	5.3	100.0
	Total	38	97.4	100.0	

Missing	No Opinion	1	2.6		
	Total	39	100.0		

Live Data Forensics

Live Data Forensics		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	19	48.7	50.0	50.0
	Important	15	38.5	39.5	89.5
	Moderately Important	4	10.3	10.5	100.0
	Total	38	97.4	100.0	
Missing	No Opinion	1	2.6		
	Total	39	100.0		

Digital Forensics Tools (Proprietary)

Digital Forensics Tools (Proprietary)		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	26	66.7	68.4	68.4
	Important	7	17.9	18.4	86.8
	Moderately Important	4	10.3	10.5	97.4
	Not Important at all	1	2.6	2.6	100.0
	Total	38	97.4	100.0	
Missing	No Opinion	1	2.6		
	Total	39	100.0		

Digital Forensics Tools (Open Source)

Digital Forensics Tools (Open Source)		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	24	61.5	63.2	63.2
	Important	10	25.6	26.3	89.5
	Moderately Important	4	10.3	10.5	100.0
	Total	38	97.4	100.0	
Missing	No Opinion	1	2.6		
	Total	39	100.0		

Linux as an Investigative Tool

Linux as an Investigative Tool		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	14	35.9	36.8	36.8
	Important	16	41.0	42.1	78.9
	Moderately Important	8	20.5	21.1	100.0
	Total	38	97.4	100.0	
Missing	No Opinion	1	2.6		
	Total	39	100.0		

Software Engineering/Development

Software Engineering/Development		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	5	12.8	12.8	12.8
	Important	8	20.5	20.5	33.3
	Moderately Important	16	41.0	41.0	74.4
	Slightly Important	8	20.5	20.5	94.9
	Not Important at all	2	5.1	5.1	100.0
	Total	39	100.0	100.0	

Scripting/Programming

Scripting/Programming		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	14	35.9	35.9	35.9
	Important	9	23.1	23.1	59.0
	Moderately Important	13	33.3	33.3	92.3
	Slightly Important	3	7.7	7.7	100.0
	Total	39	100.0	100.0	

Pen Testing Techniques and Tools

Pen Testing Techniques and Tools		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	19	48.7	48.7	48.7
	Important	13	33.3	33.3	82.1
	Moderately Important	6	15.4	15.4	97.4
	Slightly Important	1	2.6	2.6	100.0
	Total	39	100.0	100.0	

Ethical Hacking and Countermeasures

Ethical Hacking and Countermeasures		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	25	64.1	64.1	64.1
	Important	11	28.2	28.2	92.3
	Moderately Important	3	7.7	7.7	100.0
	Total	39	100.0	100.0	

Information Security and Assurance

Information Security and Assurance		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	18	46.2	46.2	46.2
	Important	18	46.2	46.2	92.3

	Moderately Important	3	7.7	7.7	100.0
	Total	39	100.0	100.0	

Server Infrastructure

Server Infrastructure		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	11	28.2	28.2	28.2
	Important	13	33.3	33.3	61.5
	Moderately Important	11	28.2	28.2	89.7
	Slightly Important	4	10.3	10.3	100.0
	Total	39	100.0	100.0	

Networks

Networks		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	21	53.8	53.8	53.8
	Important	11	28.2	28.2	82.1
	Moderately Important	6	15.4	15.4	97.4
	Slightly Important	1	2.6	2.6	100.0
	Total	39	100.0	100.0	

Databases

Databases		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	11	28.2	28.2	28.2
	Important	10	25.6	25.6	53.8
	Moderately Important	15	38.5	38.5	92.3
	Slightly Important	3	7.7	7.7	100.0
	Total	39	100.0	100.0	

Operating, File and Computer Systems

Operating, File and Computer Systems		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	18	46.2	46.2	46.2
	Important	11	28.2	28.2	74.4
	Moderately Important	8	20.5	20.5	94.9
	Slightly Important	2	5.1	5.1	100.0
	Total	39	100.0	100.0	

Cryptography

Cryptography		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	19	48.7	48.7	48.7

	Important	11	28.2	28.2	76.9
	Moderately Important	7	17.9	17.9	94.9
	Slightly Important	2	5.1	5.1	100.0
	Total	39	100.0	100.0	

Computational Mathematics

Computational Mathematics		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	6	15.4	15.8	15.8
	Important	11	28.2	28.9	44.7
	Moderately Important	12	30.8	31.6	76.3
	Slightly Important	9	23.1	23.7	100.0
	Total	38	97.4	100.0	
Missing	No Opinion	1	2.6		
Total		39	100.0		

Internet of Things

Internet of Things		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	14	35.9	35.9	35.9
	Important	12	30.8	30.8	66.7
	Moderately Important	12	30.8	30.8	97.4
	Slightly Important	1	2.6	2.6	100.0
	Total	39	100.0	100.0	

Contemporary Issues/Emerging Technologies

Contemporary Issues/Emerging Technologies		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	15	38.5	39.5	39.5
	Important	10	25.6	26.3	65.8
	Moderately Important	11	28.2	28.9	94.7
	Slightly Important	2	5.1	5.3	100.0
	Total	38	97.4	100.0	
Missing	No Opinion	1	2.6		
Total		39	100.0		

Employability Skills

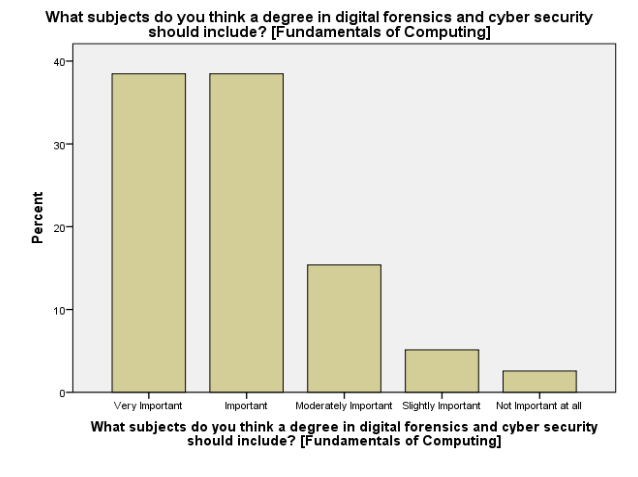
Employability Skills		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	18	46.2	46.2	46.2
	Important	10	25.6	25.6	71.8
	Moderately Important	6	15.4	15.4	87.2
	Slightly Important	4	10.3	10.3	97.4
	Not Important at all	1	2.6	2.6	100.0

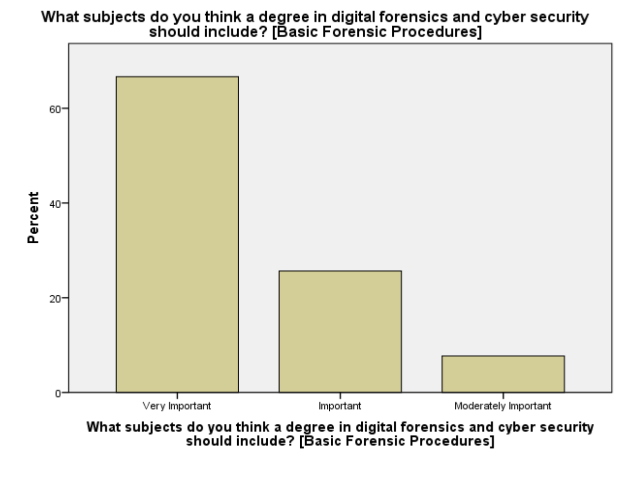
	Total	39	100.0	100.0	

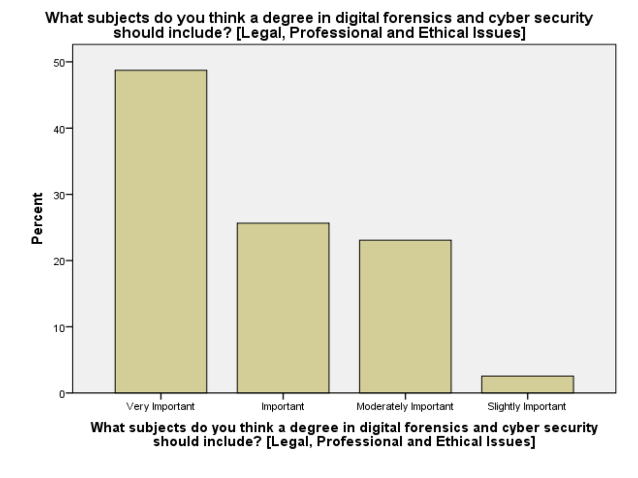
Project Management

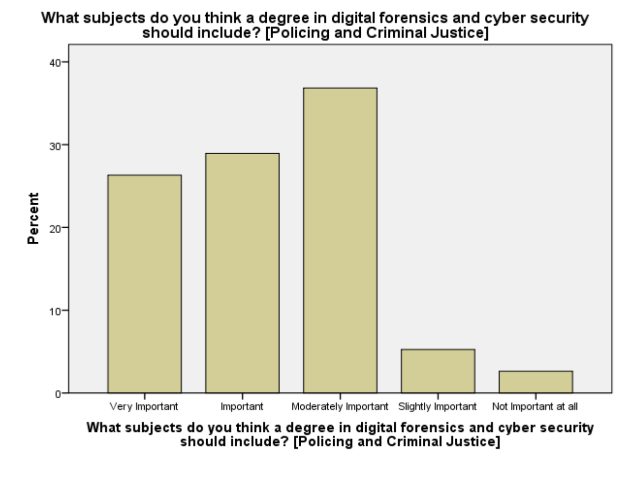
Project Management		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Important	11	28.2	28.2	28.2
	Important	12	30.8	30.8	59.0
	Moderately Important	7	17.9	17.9	76.9
	Slightly Important	3	7.7	7.7	84.6
	Not Important at all	6	15.4	15.4	100.0
	Total	39	100.0	100.0	

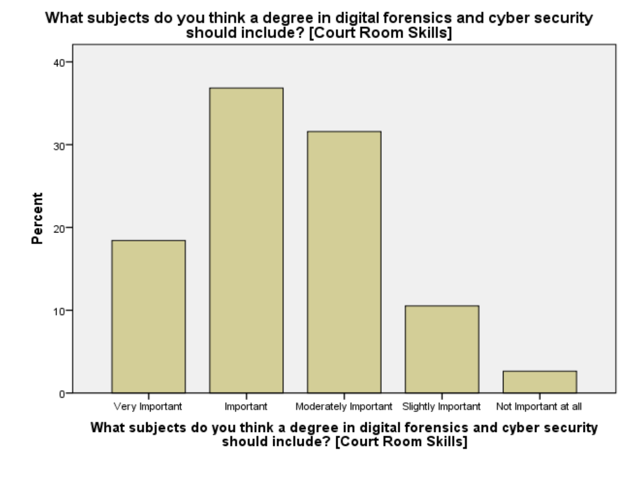
D.2.2 Frequency Statistics (per topic – all students) – SPSS Bar Charts

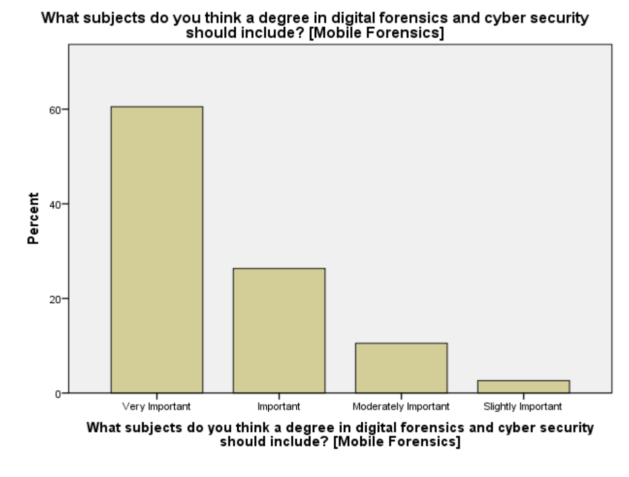


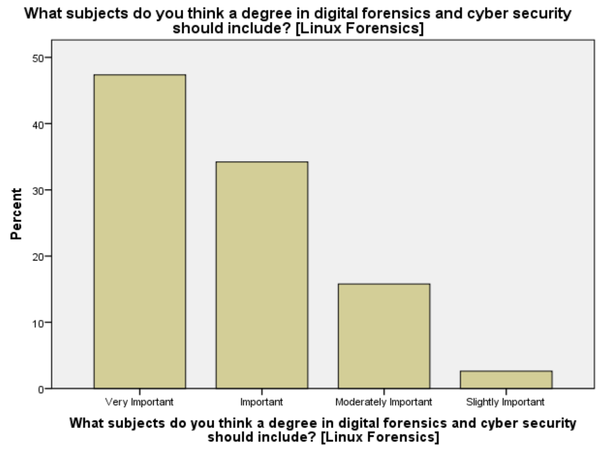


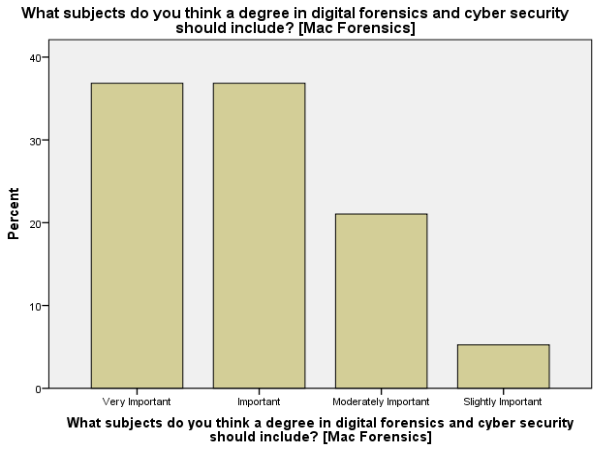


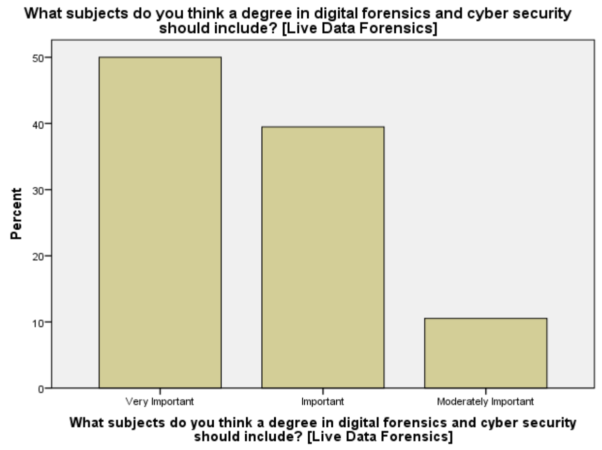


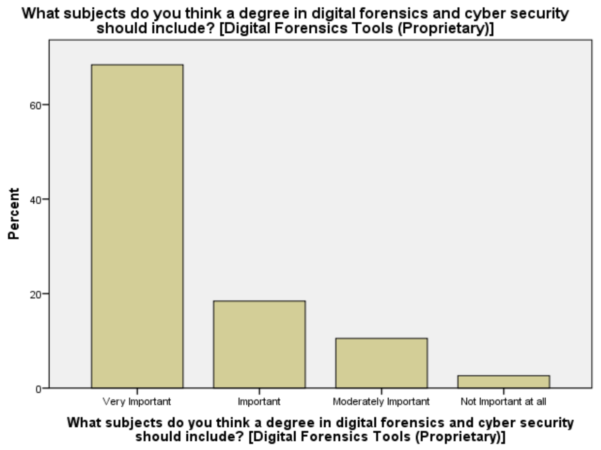


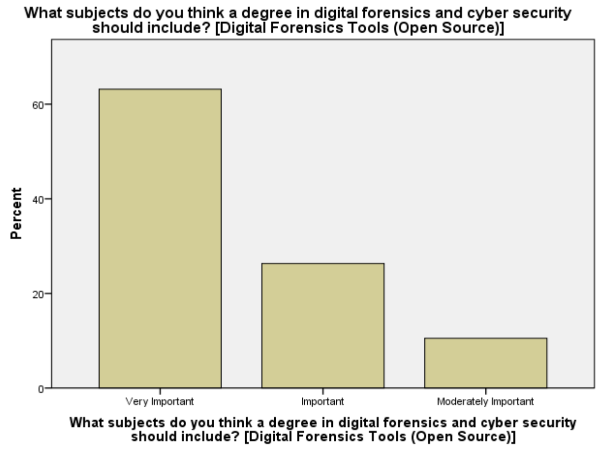


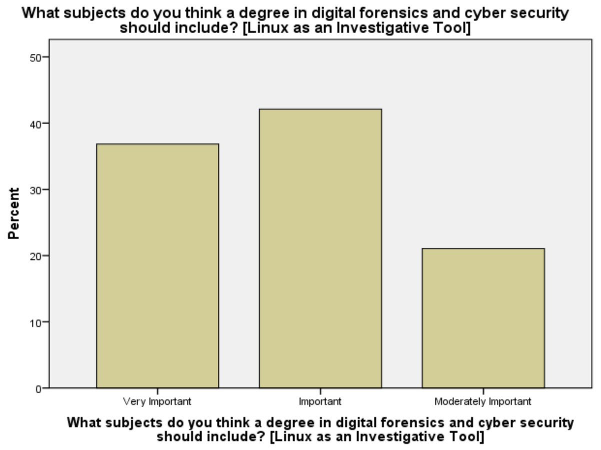

What subjects do you think a degree in digital forensics and cyber security should include? [Linux Forensics]
Percent
0
10
20
30
40
50
Very Important
Important
Moderately Important
Slightly Important
What subjects do you think a degree in digital forensics and cyber security should include? [Linux Forensics]

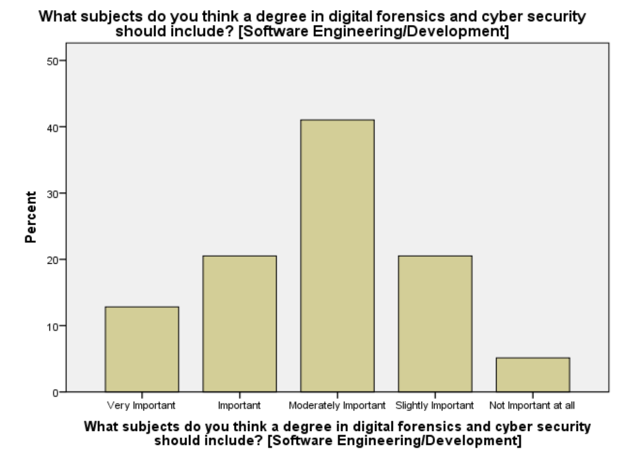

What subjects do you think a degree in digital forensics and cyber security should include? [Mac Forensics]
Percent
0
10
20
30
40
Very Important
Important
Moderately Important
Slightly Important
What subjects do you think a degree in digital forensics and cyber security should include? [Mac Forensics]

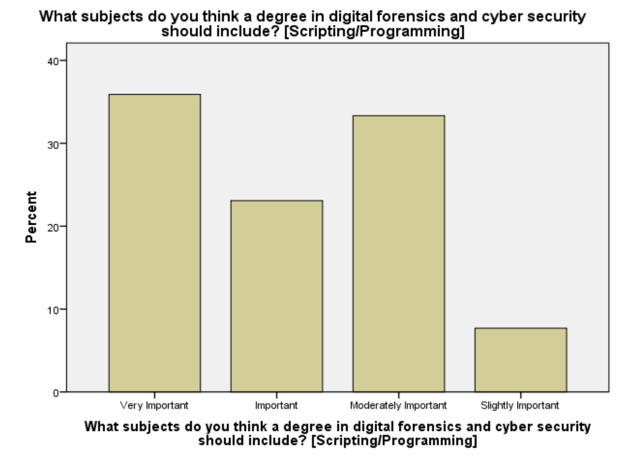

What subjects do you think a degree in digital forensics and cyber security should include? [Live Data Forensics]
Percent
0
10
20
30
40
50
Very Important
Important
Moderately Important
What subjects do you think a degree in digital forensics and cyber security should include? [Live Data Forensics]

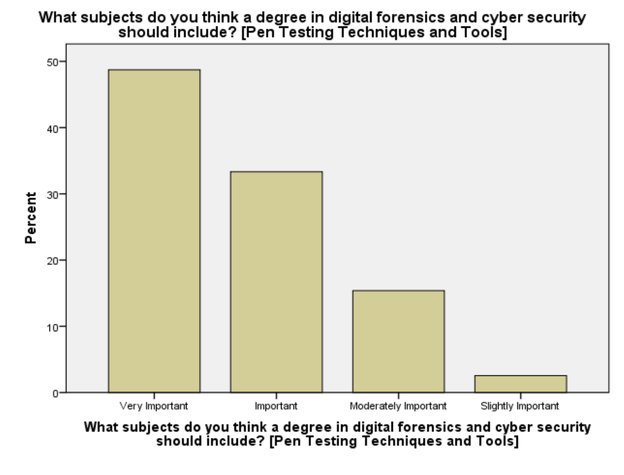

What subjects do you think a degree in digital forensics and cyber security should include? [Digital Forensics Tools (Proprietary)]
Percent
0
20
40
60
Very Important
Important
Moderately Important
Not Important at all
What subjects do you think a degree in digital forensics and cyber security should include? [Digital Forensics Tools (Proprietary)]

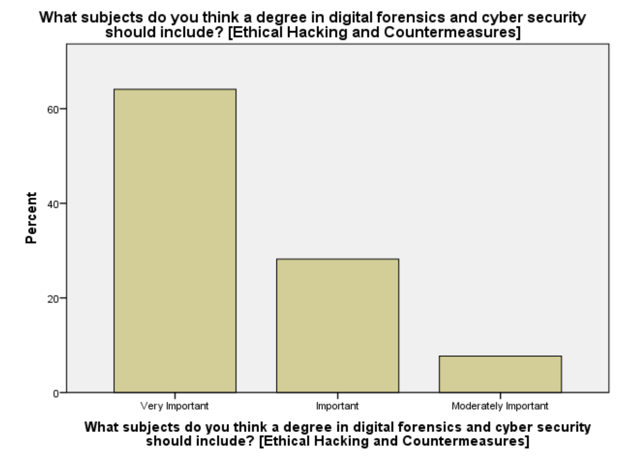

What subjects do you think a degree in digital forensics and cyber security should include? [Digital Forensics Tools (Open Source)]
Percent
0
20
40
60
Very Important
Important
Moderately Important
What subjects do you think a degree in digital forensics and cyber security should include? [Digital Forensics Tools (Open Source)]

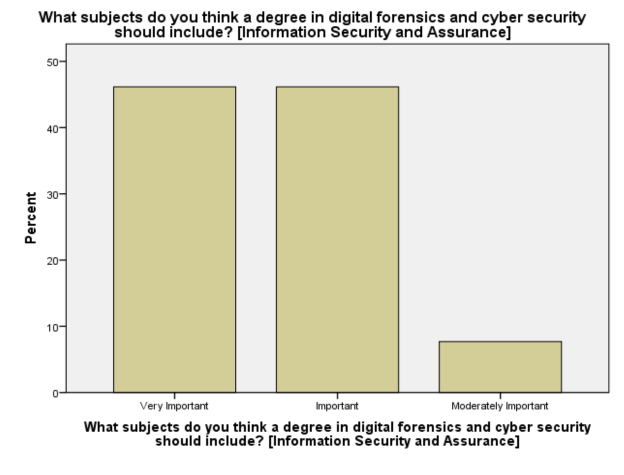

What subjects do you think a degree in digital forensics and cyber security should include? [Linux as an Investigative Tool]
Percent
0
10
20
30
40
50
Very Important
Important
Moderately Important
What subjects do you think a degree in digital forensics and cyber security should include? [Linux as an Investigative Tool]

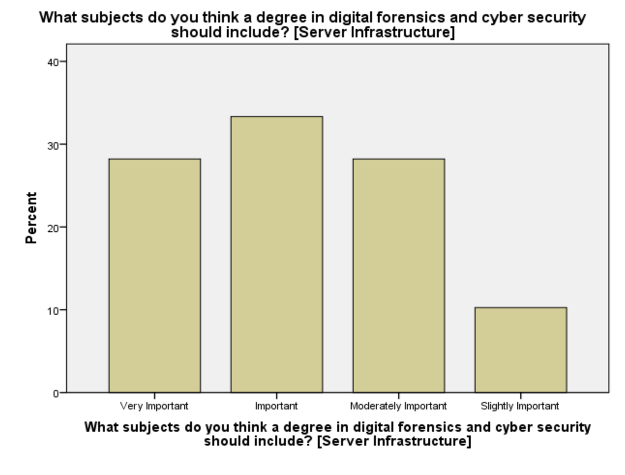

What subjects do you think a degree in digital forensics and cyber security should include? [Software Engineering/Development]
Percent
50
40
30
20
10
0
Very Important
Important
Moderately Important
Slightly Important
Not Important at all
What subjects do you think a degree in digital forensics and cyber security should include? [Software Engineering/Development]

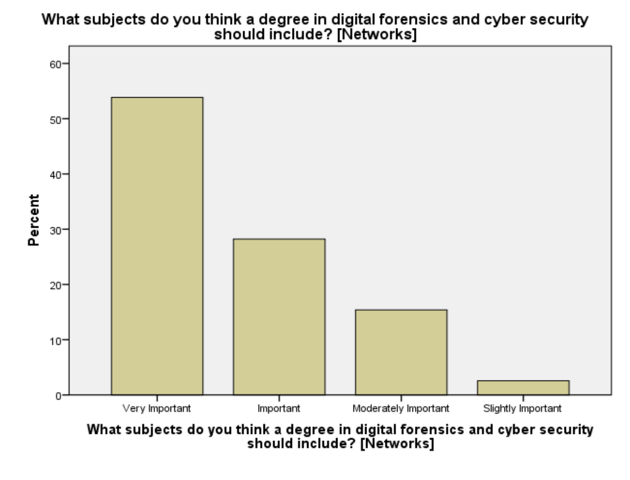

What subjects do you think a degree in digital forensics and cyber security should include? [Scripting/Programming]
Percent
40
30
20
10
0
Very Important
Important
Moderately Important
Slightly Important
What subjects do you think a degree in digital forensics and cyber security should include? [Scripting/Programming]

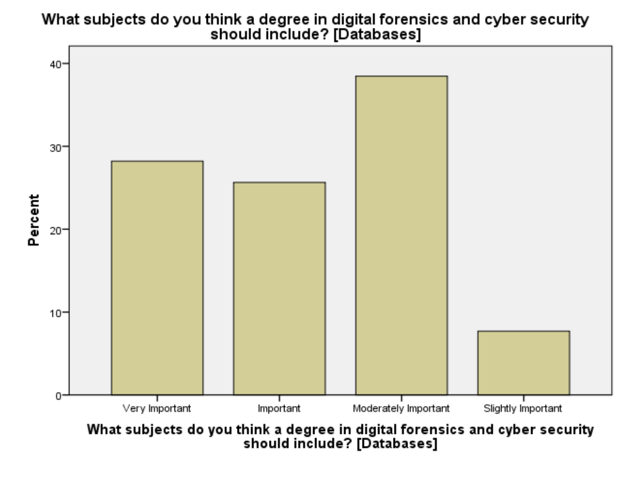

What subjects do you think a degree in digital forensics and cyber security should include? [Pen Testing Techniques and Tools]
Percent
50
40
30
20
10
0
Very Important
Important
Moderately Important
Slightly Important
What subjects do you think a degree in digital forensics and cyber security should include? [Pen Testing Techniques and Tools]

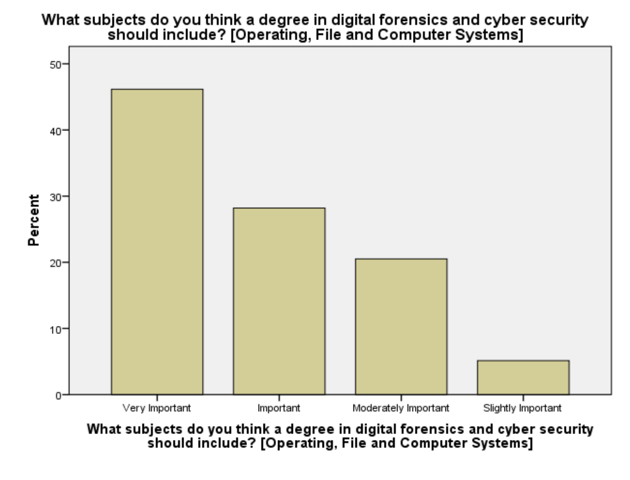

What subjects do you think a degree in digital forensics and cyber security should include? [Ethical Hacking and Countermeasures]
Percent
60
40
20
0
Very Important
Important
Moderately Important
What subjects do you think a degree in digital forensics and cyber security should include? [Ethical Hacking and Countermeasures]

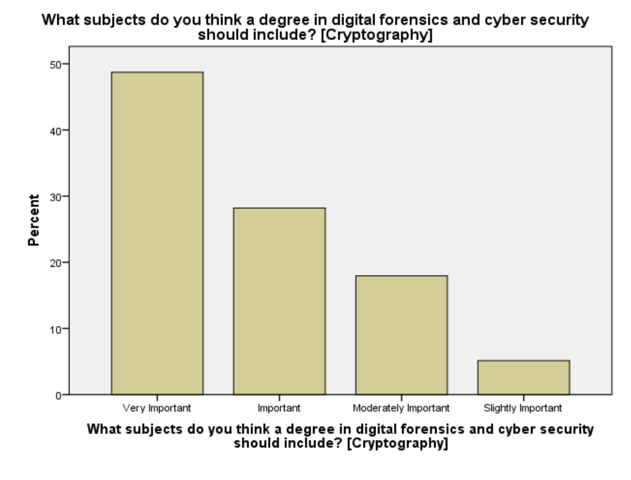

What subjects do you think a degree in digital forensics and cyber security should include? [Information Security and Assurance]
Percent
50
40
30
20
10
0
Very Important
Important
Moderately Important
What subjects do you think a degree in digital forensics and cyber security should include? [Information Security and Assurance]

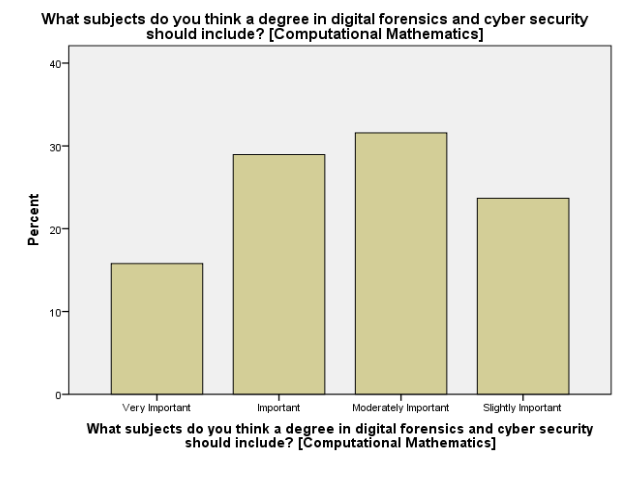

What subjects do you think a degree in digital forensics and cyber security should include? [Server Infrastructure]
Percent
40
30
20
10
0
Very Important
Important
Moderately Important
Slightly Important
What subjects do you think a degree in digital forensics and cyber security should include? [Server Infrastructure]

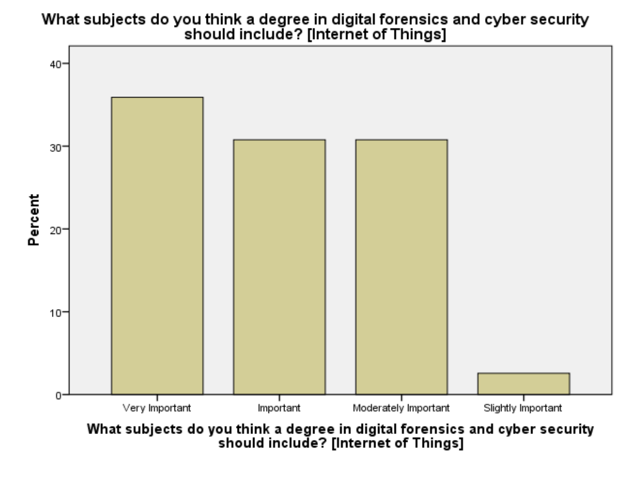

What subjects do you think a degree in digital forensics and cyber security should include? [Networks]
Percent
60
50
40
30
20
10
0
Very Important
Important
Moderately Important
Slightly Important
What subjects do you think a degree in digital forensics and cyber security should include? [Networks]

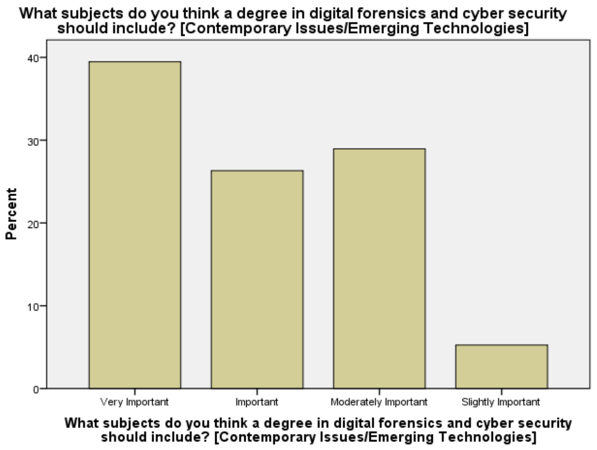

What subjects do you think a degree in digital forensics and cyber security should include? [Databases]
Percent
40
30
20
10
0
Very Important
Important
Moderately Important
Slightly Important
What subjects do you think a degree in digital forensics and cyber security should include? [Databases]

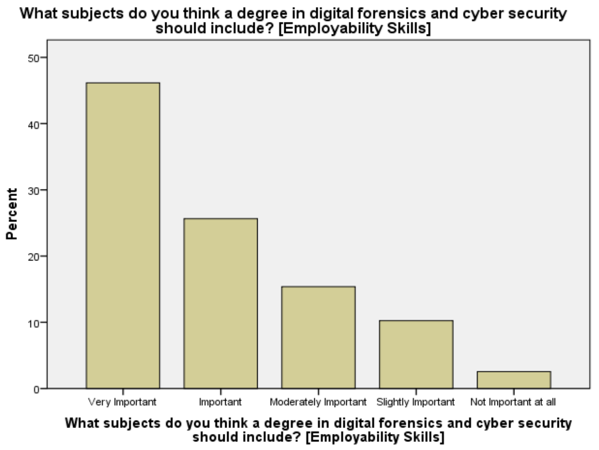

What subjects do you think a degree in digital forensics and cyber security should include? [Operating, File and Computer Systems]
Percent
50
40
30
20
10
0
Very Important
Important
Moderately Important
Slightly Important
What subjects do you think a degree in digital forensics and cyber security should include? [Operating, File and Computer Systems]

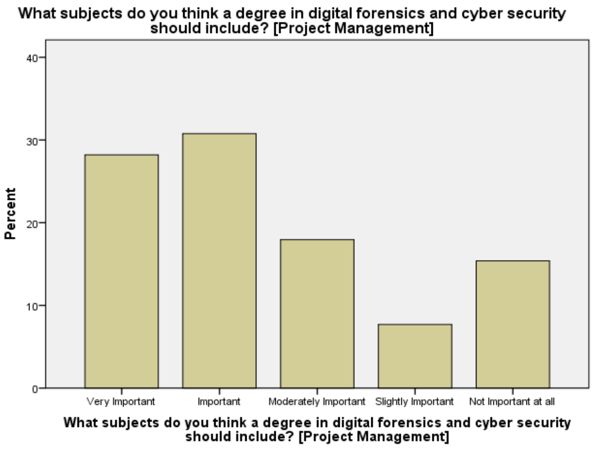

What subjects do you think a degree in digital forensics and cyber security should include? [Cryptography]
Percent
50
40
30
20
10
0
Very Important
Important
Moderately Important
Slightly Important
What subjects do you think a degree in digital forensics and cyber security should include? [Cryptography]


What subjects do you think a degree in digital forensics and cyber security should include? [Computational Mathematics]
Percent
40
30
20
10
0
Very Important
Important
Moderately Important
Slightly Important
What subjects do you think a degree in digital forensics and cyber security should include? [Computational Mathematics]


What subjects do you think a degree in digital forensics and cyber security should include? [Internet of Things]
Percent
40
30
20
10
0
Very Important
Important
Moderately Important
Slightly Important
What subjects do you think a degree in digital forensics and cyber security should include? [Internet of Things]







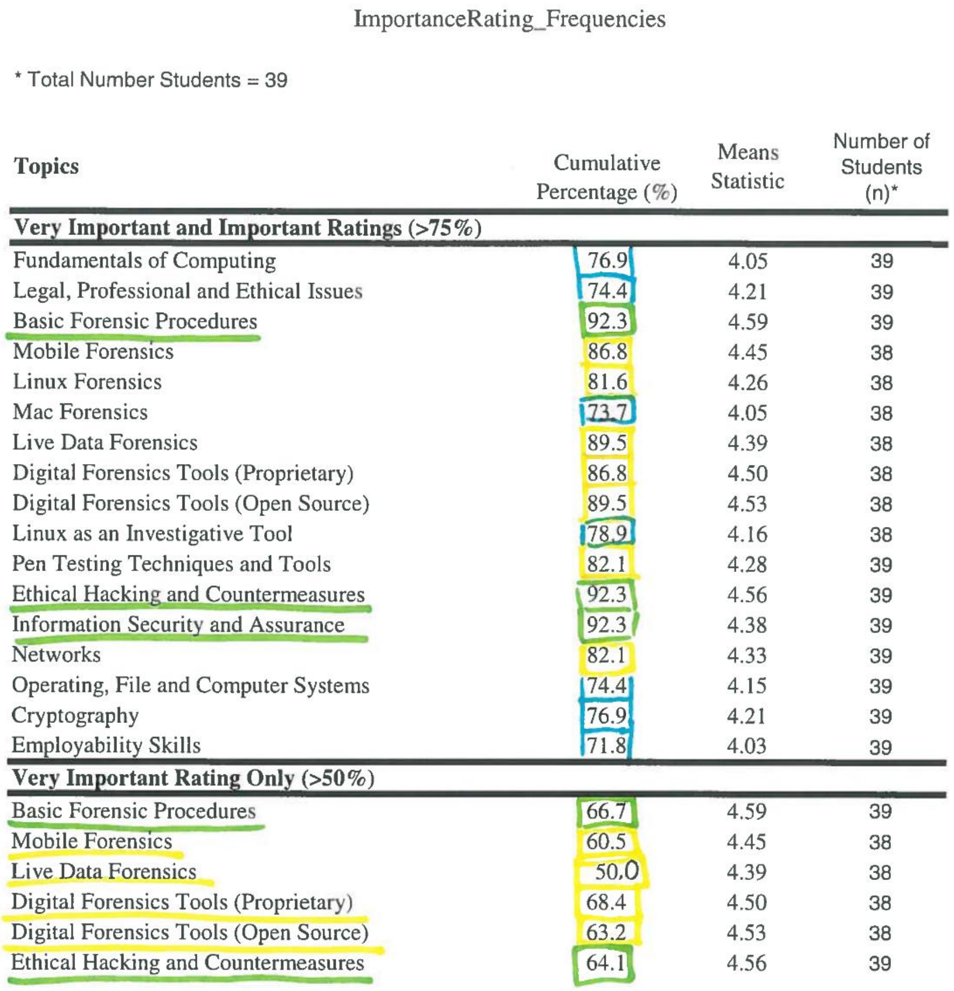
D.2.3 Workings out to identifying topics by importance by ratings (per topic and workshop group)

Within this section tables are presented which demonstrate which topics were important, and how they were rated, by all students (n=39) as well as per workshop group (n=16 or n=23) presented in chapter 6.

The following Key represents the colour system used within figures in the section. Each relates to a different percentile bracket to identify those rated most important based on frequency statistics. The Cumulative percentiles correspond to ‘Very Important’ and ‘Important’ where the percentile is above 75 percent and for ‘Very Important’ when the ratings accounted for greater than 50 percent.

Topics	Cumulative Percentage (%)	Means Statistic	Number of Students (n)*
Very Important and Important Ratings (>75%)			
Basic Forensic Procedures	92.3	4.59	39
Ethical Hacking and Countermeasures	92.3	4.56	39
Information Security and Assurance	92.3	4.38	39
Live Data Forensics	89.5	4.39	38
Digital Forensics Tools (Open Source)	89.5	4.53	38
Mobile Forensics	86.8	4.45	38
Digital Forensics Tools (Proprietary)	86.8	4.50	38
Pen Testing Techniques and Tools	82.1	4.28	39
Networks	82.1	4.33	39
Linux Forensics	81.6	4.26	38
Linux as an Investigative Tool	78.9	4.16	38
Fundamentals of Computing	76.9	4.05	39
Cryptography	76.9	4.21	39
Legal, Professional and Ethical Issues	74.4	4.21	39
Operating, File and Computer Systems	74.4	4.15	39
Mac Forensics	73.7	4.05	38
Employability Skills	71.8	4.03	39
Very Important Rating Only (>50%)			
Digital Forensics Tools (Proprietary)	68.4	4.50	38
Basic Forensic Procedures	66.7	4.59	39
Ethical Hacking and Countermeasures	64.1	4.56	39
Digital Forensics Tools (Open Source)	63.2	4.53	38
Mobile Forensics	60.5	4.45	38
Live Data Forensics	50.0	4.39	38

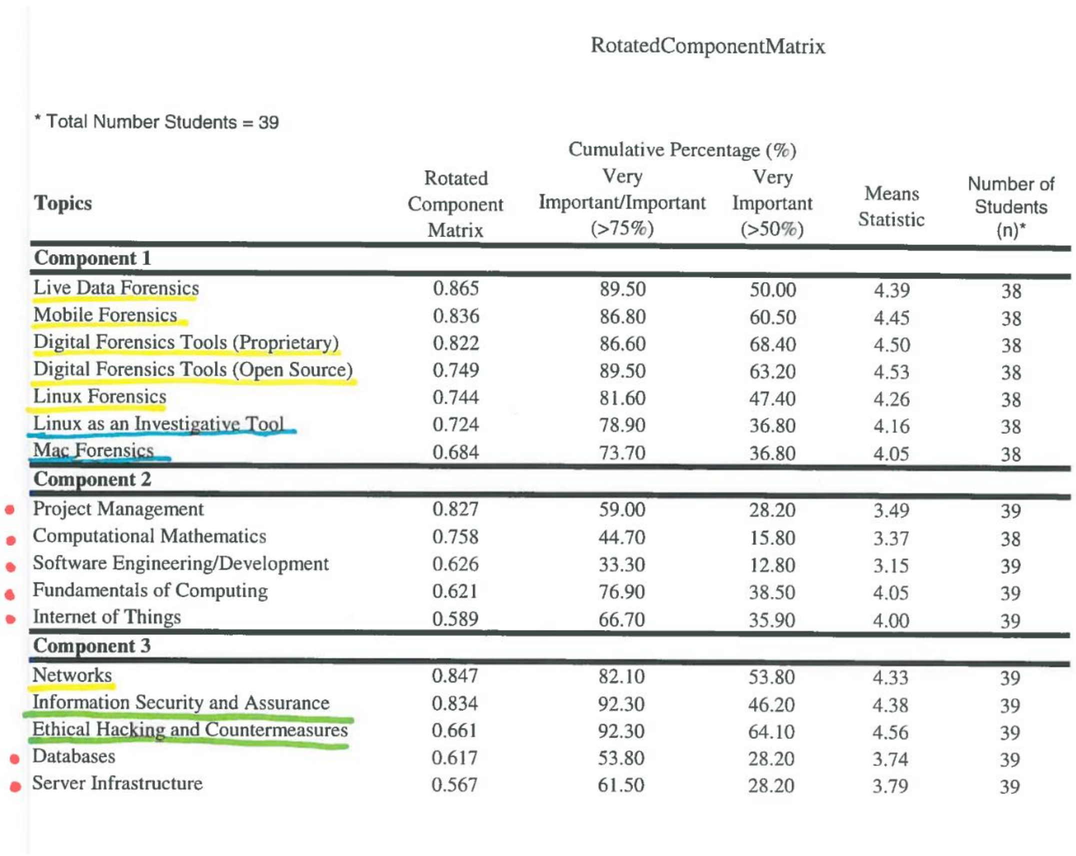
* Total Number of Students (n) = 39



ImportanceRating_Frequencies

* Total Number Students = 39

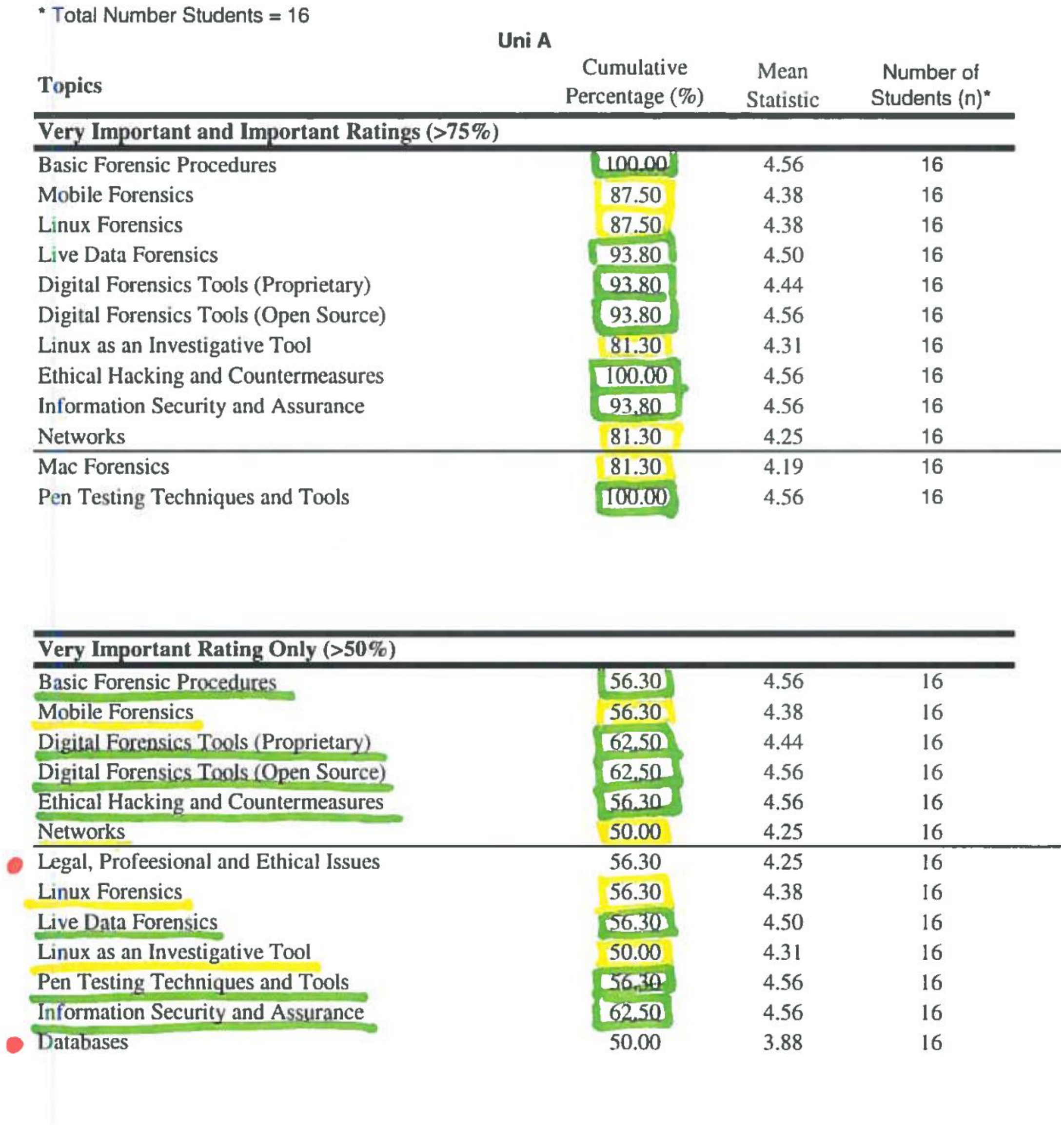
Topics	Cumulative Percentage (%)	Means Statistic	Number of Students (n)*
Very Important and Important Ratings (>75%)			
Fundamentals of Computing	76.9	4.05	39
Legal, Professional and Ethical Issues	74.4	4.21	39
Basic Forensic Procedures	92.3	4.59	39
Mobile Forensics	86.8	4.45	38
Linux Forensics	81.6	4.26	38
Mac Forensics	73.7	4.05	38
Live Data Forensics	89.5	4.39	38
Digital Forensics Tools (Proprietary)	86.8	4.50	38
Digital Forensics Tools (Open Source)	89.5	4.53	38
Linux as an Investigative Tool	78.9	4.16	38
Pen Testing Techniques and Tools	82.1	4.28	39
Ethical Hacking and Countermeasures	92.3	4.56	39
Information Security and Assurance	92.3	4.38	39
Networks	82.1	4.33	39
Operating, File and Computer Systems	74.4	4.15	39
Cryptography	76.9	4.21	39
Employability Skills	71.8	4.03	39
Very Important Rating Only (>50%)			
Basic Forensic Procedures	66.7	4.59	39
Mobile Forensics	60.5	4.45	38
Live Data Forensics	50.0	4.39	38
Digital Forensics Tools (Proprietary)	68.4	4.50	38
Digital Forensics Tools (Open Source)	63.2	4.53	38
Ethical Hacking and Countermeasures	64.1	4.56	39



RotatedComponentMatrix

* Total Number Students = 39

Topics	Rotated Component Matrix	Cumulative Percentage (%) Very Important/Important (>75%)	Very Important (>50%)	Means Statistic	Number of Students (n)*
Component 1					
Live Data Forensics	0.865	89.50	50.00	4.39	38
Mobile Forensics	0.836	86.80	60.50	4.45	38
Digital Forensics Tools (Proprietary)	0.822	86.60	68.40	4.50	38
Digital Forensics Tools (Open Source)	0.749	89.50	63.20	4.53	38
Linux Forensics	0.744	81.60	47.40	4.26	38
Linux as an Investigative Tool	0.724	78.90	36.80	4.16	38
Mac Forensics	0.684	73.70	36.80	4.05	38
Component 2					
● Project Management	0.827	59.00	28.20	3.49	39
● Computational Mathematics	0.758	44.70	15.80	3.37	38
● Software Engineering/Development	0.626	33.30	12.80	3.15	39
● Fundamentals of Computing	0.621	76.90	38.50	4.05	39
● Internet of Things	0.589	66.70	35.90	4.00	39
Component 3					
Networks	0.847	82.10	53.80	4.33	39
Information Security and Assurance	0.834	92.30	46.20	4.38	39
Ethical Hacking and Countermeasures	0.661	92.30	64.10	4.56	39
● Databases	0.617	53.80	28.20	3.74	39
● Server Infrastructure	0.567	61.50	28.20	3.79	39

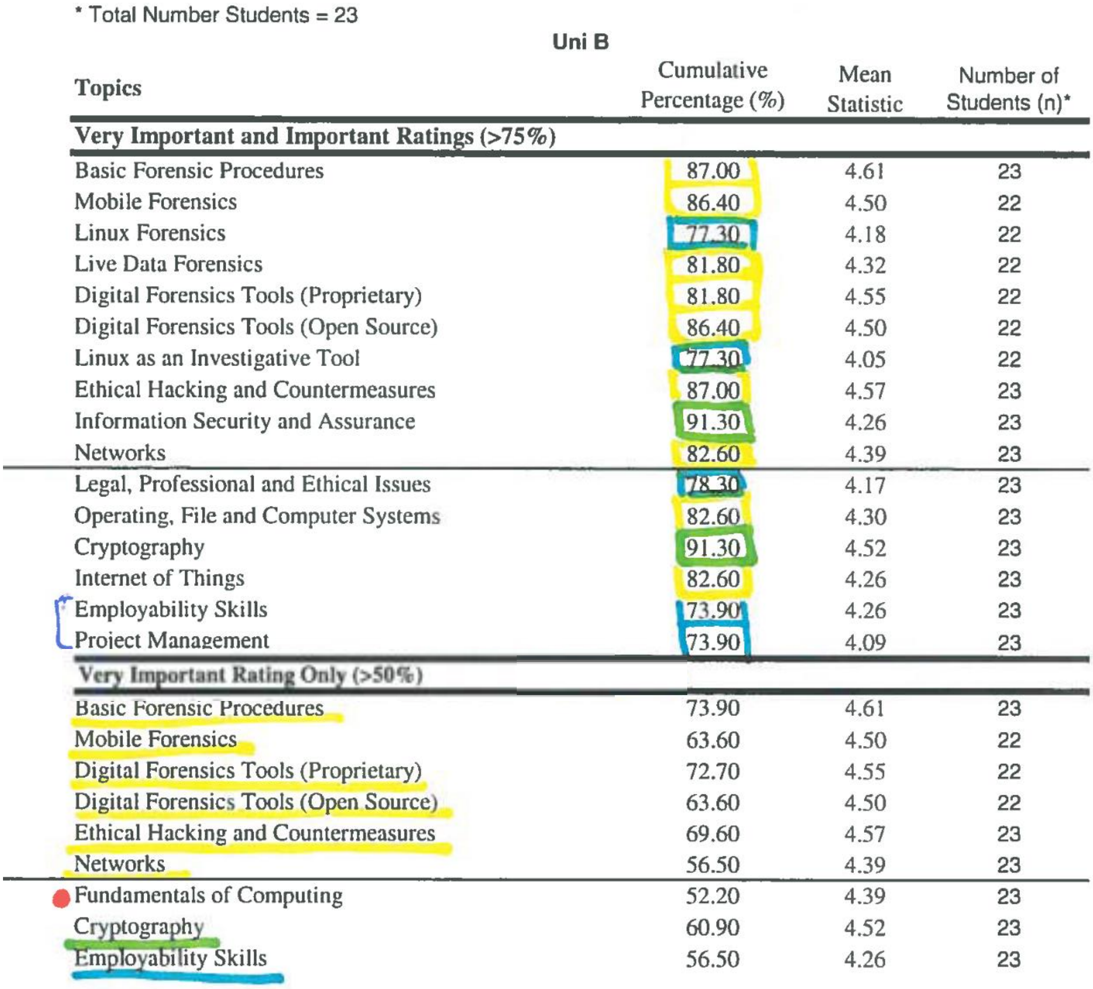


* Total Number Students = 16

Uni A

Topics	Cumulative Percentage (%)	Mean Statistic	Number of Students (n)*
Very Important and Important Ratings (>75%)			
Basic Forensic Procedures	100.00	4.56	16
Mobile Forensics	87.50	4.38	16
Linux Forensics	87.50	4.38	16
Live Data Forensics	93.80	4.50	16
Digital Forensics Tools (Proprietary)	93.80	4.44	16
Digital Forensics Tools (Open Source)	93.80	4.56	16
Linux as an Investigative Tool	81.30	4.31	16
Ethical Hacking and Countermeasures	100.00	4.56	16
Information Security and Assurance	93.80	4.56	16
Networks	81.30	4.25	16
Mac Forensics	81.30	4.19	16
Pen Testing Techniques and Tools	100.00	4.56	16

Topics	Cumulative Percentage (%)	Mean Statistic	Number of Students (n)*
Very Important Rating Only (>50%)			
Basic Forensic Procedures	56.30	4.56	16
Mobile Forensics	56.30	4.38	16
Digital Forensics Tools (Proprietary)	62.50	4.44	16
Digital Forensics Tools (Open Source)	62.50	4.56	16
Ethical Hacking and Countermeasures	56.30	4.56	16
Networks	50.00	4.25	16
Legal, Profeesional and Ethical Issues	56.30	4.25	16
Linux Forensics	56.30	4.38	16
Live Data Forensics	56.30	4.50	16
Linux as an Investigative Tool	50.00	4.31	16
Pen Testing Techniques and Tools	56.30	4.56	16
Information Security and Assurance	62.50	4.56	16
Databases	50.00	3.88	16



* Total Number Students = 23

Uni B

Topics	Cumulative Percentage (%)	Mean Statistic	Number of Students (n)*
Very Important and Important Ratings (>75%)			
Basic Forensic Procedures	87.00	4.61	23
Mobile Forensics	86.40	4.50	22
Linux Forensics	77.30	4.18	22
Live Data Forensics	81.80	4.32	22
Digital Forensics Tools (Proprietary)	81.80	4.55	22
Digital Forensics Tools (Open Source)	86.40	4.50	22
Linux as an Investigative Tool	77.30	4.05	22
Ethical Hacking and Countermeasures	87.00	4.57	23
Information Security and Assurance	91.30	4.26	23
Networks	82.60	4.39	23
Legal, Professional and Ethical Issues	78.30	4.17	23
Operating, File and Computer Systems	82.60	4.30	23
Cryptography	91.30	4.52	23
Internet of Things	82.60	4.26	23
Employability Skills	73.90	4.26	23
Project Management	73.90	4.09	23
Very Important Rating Only (>50%)			
Basic Forensic Procedures	73.90	4.61	23
Mobile Forensics	63.60	4.50	22
Digital Forensics Tools (Proprietary)	72.70	4.55	22
Digital Forensics Tools (Open Source)	63.60	4.50	22
Ethical Hacking and Countermeasures	69.60	4.57	23
Networks	56.50	4.39	23
● Fundamentals of Computing	52.20	4.39	23
Cryptography	60.90	4.52	23
Employability Skills	56.50	4.26	23

D.2.4 Frequency Statistics (per group) – SPSS

This section highlights topics/skills students were asked to rate based on workshop/group of students. This data was used in chapter 6 to present findings relating to difference in views among students across both groups.

Fundamentals of Computing

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	3	18.8	18.8	18.8
		Important	7	43.8	43.8	62.5
		Moderately Important	3	18.8	18.8	81.3
		Slightly Important	2	12.5	12.5	93.8
		Not Important at all	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	12	52.2	52.2	52.2
		Important	8	34.8	34.8	87.0
		Moderately Important	3	13.0	13.0	100.0
		Total	23	100.0	100.0	

Basic Forensic Procedures

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	9	56.3	56.3	56.3
		Important	7	43.8	43.8	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	17	73.9	73.9	73.9
		Important	3	13.0	13.0	87.0
		Moderately Important	3	13.0	13.0	100.0
		Total	23	100.0	100.0	

Legal, Professional and Ethical Issues

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	9	56.3	56.3	56.3
		Important	2	12.5	12.5	68.8
		Moderately Important	5	31.3	31.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	10	43.5	43.5	43.5
		Important	8	34.8	34.8	78.3
		Moderately Important	4	17.4	17.4	95.7

		Slightly Important	1	4.3	4.3	100.0
		Total	23	100.0	100.0	

Policing and Criminal Justice

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	5	31.3	31.3	31.3
		Important	4	25.0	25.0	56.3
		Moderately Important	6	37.5	37.5	93.8
		Not Important at all	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	5	21.7	22.7	22.7
		Important	7	30.4	31.8	54.5
		Moderately Important	8	34.8	36.4	90.9
		Slightly Important	2	8.7	9.1	100.0
		Total	22	95.7	100.0	
	Missing	No Opinion	1	4.3		
	Total		23	100.0		

Court Room Skills

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	3	18.8	18.8	18.8
		Important	6	37.5	37.5	56.3
		Moderately Important	6	37.5	37.5	93.8
		Not Important at all	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	4	17.4	18.2	18.2
		Important	8	34.8	36.4	54.5
		Moderately Important	6	26.1	27.3	81.8
		Slightly Important	4	17.4	18.2	100.0
		Total	22	95.7	100.0	
	Missing	No Opinion	1	4.3		
	Total		23	100.0		

Mobile Forensics

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	9	56.3	56.3	56.3
		Important	5	31.3	31.3	87.5
		Moderately Important	1	6.3	6.3	93.8
		Slightly Important	1	6.3	6.3	100.0

		Total	16	100.0	100.0	
2	Valid	Very Important	14	60.9	63.6	63.6
		Important	5	21.7	22.7	86.4
		Moderately Important	3	13.0	13.6	100.0
		Total	22	95.7	100.0	
	Missing	No Opinion	1	4.3		
	Total		23	100.0		

Linux Forensics

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	9	56.3	56.3	56.3
		Important	5	31.3	31.3	87.5
		Moderately Important	1	6.3	6.3	93.8
		Slightly Important	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	9	39.1	40.9	40.9
		Important	8	34.8	36.4	77.3
		Moderately Important	5	21.7	22.7	100.0
		Total	22	95.7	100.0	
	Missing	No Opinion	1	4.3		
	Total		23	100.0		

Mac Forensics

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	7	43.8	43.8	43.8
		Important	6	37.5	37.5	81.3
		Moderately Important	2	12.5	12.5	93.8
		Slightly Important	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	7	30.4	31.8	31.8
		Important	8	34.8	36.4	68.2
		Moderately Important	6	26.1	27.3	95.5
		Slightly Important	1	4.3	4.5	100.0
		Total	22	95.7	100.0	
	Missing	No Opinion	1	4.3		
	Total		23	100.0		

Live Data Forensics

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	9	56.3	56.3	56.3
		Important	6	37.5	37.5	93.8
		Moderately Important	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	10	43.5	45.5	45.5
		Important	9	39.1	40.9	86.4
		Moderately Important	3	13.0	13.6	100.0
		Total	22	95.7	100.0	
	Missing	No Opinion	1	4.3		
	Total		23	100.0		

Digital Forensics Tools (Proprietary)

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	10	62.5	62.5	62.5
		Important	5	31.3	31.3	93.8
		Not Important at all	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	16	69.6	72.7	72.7
		Important	2	8.7	9.1	81.8
		Moderately Important	4	17.4	18.2	100.0
		Total	22	95.7	100.0	
	Missing	No Opinion	1	4.3		
	Total		23	100.0		

Digital Forensics Tools (Open Source)

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	10	62.5	62.5	62.5
		Important	5	31.3	31.3	93.8
		Moderately Important	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	14	60.9	63.6	63.6
		Important	5	21.7	22.7	86.4
		Moderately Important	3	13.0	13.6	100.0
		Total	22	95.7	100.0	
	Missing	No Opinion	1	4.3		
	Total		23	100.0		

Linux as an Investigative Tool

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	8	50.0	50.0	50.0
		Important	5	31.3	31.3	81.3
		Moderately Important	3	18.8	18.8	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	6	26.1	27.3	27.3
		Important	11	47.8	50.0	77.3
		Moderately Important	5	21.7	22.7	100.0
		Total	22	95.7	100.0	
	Missing	No Opinion	1	4.3		
	Total		23	100.0		

Software Engineering/Development

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	2	12.5	12.5	12.5
		Important	2	12.5	12.5	25.0
		Moderately Important	6	37.5	37.5	62.5
		Slightly Important	4	25.0	25.0	87.5
		Not Important at all	2	12.5	12.5	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	3	13.0	13.0	13.0
		Important	6	26.1	26.1	39.1
		Moderately Important	10	43.5	43.5	82.6
		Slightly Important	4	17.4	17.4	100.0
		Total	23	100.0	100.0	

Scripting/Programming

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	5	31.3	31.3	31.3
		Important	4	25.0	25.0	56.3
		Moderately Important	6	37.5	37.5	93.8
		Slightly Important	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	9	39.1	39.1	39.1
		Important	5	21.7	21.7	60.9
		Moderately Important	7	30.4	30.4	91.3
		Slightly Important	2	8.7	8.7	100.0

		Total	23	100.0	100.0	

Pen Testing Techniques and Tools

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	9	56.3	56.3	56.3
		Important	7	43.8	43.8	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	10	43.5	43.5	43.5
		Important	6	26.1	26.1	69.6
		Moderately Important	6	26.1	26.1	95.7
		Slightly Important	1	4.3	4.3	100.0
		Total	23	100.0	100.0	

Ethical Hacking and Countermeasures

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	9	56.3	56.3	56.3
		Important	7	43.8	43.8	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	16	69.6	69.6	69.6
		Important	4	17.4	17.4	87.0
		Moderately Important	3	13.0	13.0	100.0
		Total	23	100.0	100.0	

Information Security and Assurance

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	10	62.5	62.5	62.5
		Important	5	31.3	31.3	93.8
		Moderately Important	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	8	34.8	34.8	34.8
		Important	13	56.5	56.5	91.3
		Moderately Important	2	8.7	8.7	100.0
		Total	23	100.0	100.0	

Server Infrastructure

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	4	25.0	25.0	25.0
		Important	4	25.0	25.0	50.0
		Moderately Important	5	31.3	31.3	81.3
		Slightly Important	3	18.8	18.8	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	7	30.4	30.4	30.4
		Important	9	39.1	39.1	69.6
		Moderately Important	6	26.1	26.1	95.7
		Slightly Important	1	4.3	4.3	100.0
		Total	23	100.0	100.0	

Networks

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	8	50.0	50.0	50.0
		Important	5	31.3	31.3	81.3
		Moderately Important	2	12.5	12.5	93.8
		Slightly Important	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	13	56.5	56.5	56.5
		Important	6	26.1	26.1	82.6
		Moderately Important	4	17.4	17.4	100.0
		Total	23	100.0	100.0	

Databases

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	8	50.0	50.0	50.0
		Important	1	6.3	6.3	56.3
		Moderately Important	4	25.0	25.0	81.3
		Slightly Important	3	18.8	18.8	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	3	13.0	13.0	13.0
		Important	9	39.1	39.1	52.2
		Moderately Important	11	47.8	47.8	100.0
		Total	23	100.0	100.0	

Operating, File and Computer Systems

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	7	43.8	43.8	43.8
		Important	3	18.8	18.8	62.5
		Moderately Important	4	25.0	25.0	87.5
		Slightly Important	2	12.5	12.5	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	11	47.8	47.8	47.8
		Important	8	34.8	34.8	82.6
		Moderately Important	4	17.4	17.4	100.0
		Total	23	100.0	100.0	

Cryptography

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	5	31.3	31.3	31.3
		Important	4	25.0	25.0	56.3
		Moderately Important	5	31.3	31.3	87.5
		Slightly Important	2	12.5	12.5	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	14	60.9	60.9	60.9
		Important	7	30.4	30.4	91.3
		Moderately Important	2	8.7	8.7	100.0
		Total	23	100.0	100.0	

Computational Mathematics

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	2	12.5	12.5	12.5
		Important	2	12.5	12.5	25.0
		Moderately Important	5	31.3	31.3	56.3
		Slightly Important	7	43.8	43.8	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	4	17.4	18.2	18.2
		Important	9	39.1	40.9	59.1
		Moderately Important	7	30.4	31.8	90.9
		Slightly Important	2	8.7	9.1	100.0
		Total	22	95.7	100.0	
	Missing	No Opinion	1	4.3		
	Total		23	100.0		

Internet of Things

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	4	25.0	25.0	25.0
		Important	3	18.8	18.8	43.8
		Moderately Important	8	50.0	50.0	93.8
		Slightly Important	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	10	43.5	43.5	43.5
		Important	9	39.1	39.1	82.6
		Moderately Important	4	17.4	17.4	100.0
		Total	23	100.0	100.0	

Contemporary Issues/Emerging Technologies

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	5	31.3	31.3	31.3
		Important	5	31.3	31.3	62.5
		Moderately Important	4	25.0	25.0	87.5
		Slightly Important	2	12.5	12.5	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	10	43.5	45.5	45.5
		Important	5	21.7	22.7	68.2
		Moderately Important	7	30.4	31.8	100.0
		Total	22	95.7	100.0	
	Missing	No Opinion	1	4.3		
	Total		23	100.0		

Employability Skills

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	5	31.3	31.3	31.3
		Important	6	37.5	37.5	68.8
		Moderately Important	1	6.3	6.3	75.0
		Slightly Important	3	18.8	18.8	93.8
		Not Important at all	1	6.3	6.3	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	13	56.5	56.5	56.5
		Important	4	17.4	17.4	73.9
		Moderately Important	5	21.7	21.7	95.7
		Slightly Important	1	4.3	4.3	100.0
		Total	23	100.0	100.0	

Project Management

Group			Frequency	Percent	Valid Percent	Cumulative Percent
1	Valid	Very Important	2	12.5	12.5	12.5
		Important	4	25.0	25.0	37.5
		Moderately Important	2	12.5	12.5	50.0
		Slightly Important	2	12.5	12.5	62.5
		Not Important at all	6	37.5	37.5	100.0
		Total	16	100.0	100.0	
2	Valid	Very Important	9	39.1	39.1	39.1
		Important	8	34.8	34.8	73.9
		Moderately Important	5	21.7	21.7	95.7
		Slightly Important	1	4.3	4.3	100.0
		Total	23	100.0	100.0	

D.3 Principal Component Analysis – SPSS

As described in the methodology two tests were performed to check suitability of the data for Factor Analysis. These were: Kaiser-Meyer-Olkin Measure of Sampling Adequacy and Bartlett's Test of Sphericity (shown directly below).

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.430
Bartlett's Test of Sphericity	Approx. Chi-Square	775.307
	df	351
	Sig.	.000

This section continues by demonstrating communalities, scree plot results as well as rotated matrices considered for results in chapter 6 when using IBM SPSS Statistics 24 for all students across all workshops.

Communalities

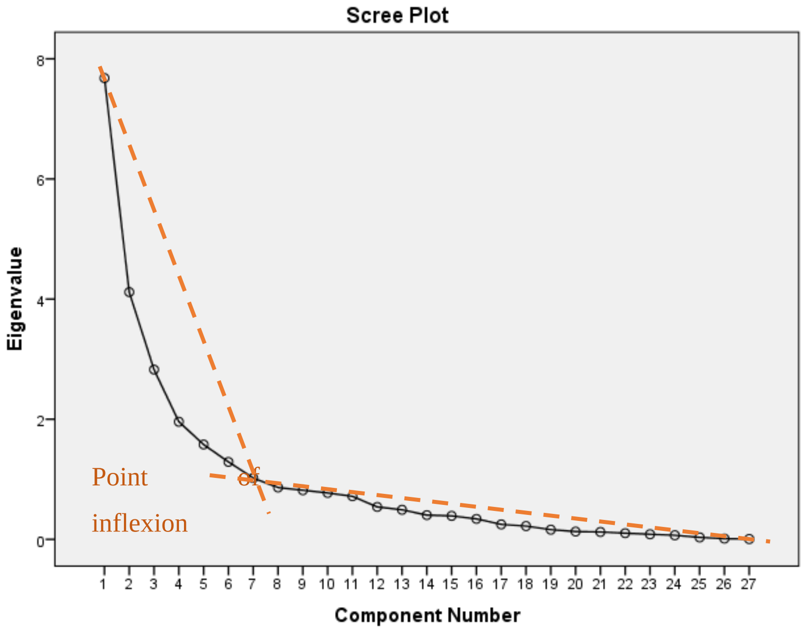
	Initial	Extraction
Fundamentals of Computing	1.000	0.709
Basic Forensic Procedures	1.000	0.765
Legal, Professional and Ethical Issues	1.000	0.817
Policing and Criminal Justice	1.000	0.834
Court Room Skills	1.000	0.677
Mobile Forensics	1.000	0.832
Linux Forensics	1.000	0.792
Mac Forensics	1.000	0.748
Live Data Forensics	1.000	0.859
Digital Forensics Tools (Proprietary)	1.000	0.754
Digital Forensics Tools (Open Source)	1.000	0.778
Linux as an Investigative Tool	1.000	0.571
Software Engineering/Development	1.000	0.742
Scripting/Programming	1.000	0.776
Pen Testing Techniques and Tools	1.000	0.782
Ethical Hacking and Countermeasures	1.000	0.755
Information Security and Assurance	1.000	0.756
Server Infrastructure	1.000	0.796
Networks	1.000	0.836
Databases	1.000	0.775
Operating, File and Computer Systems	1.000	0.792
Cryptography	1.000	0.469
Computational Mathematics	1.000	0.754
Internet of Things	1.000	0.739
Contemporary Issues/Emerging Technologies	1.000	0.767
Employability Skills	1.000	0.764
Project Management	1.000	0.830

Extraction Method: Principal Component Analysis.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	7.679	28.442	28.442	7.679	28.442	28.442	5.059	18.736	18.736
2	4.117	15.247	43.689	4.117	15.247	43.689	3.663	13.567	32.303
3	2.827	10.470	54.160	2.827	10.470	54.160	3.446	12.765	45.067
4	1.958	7.250	61.410	1.958	7.250	61.410	2.671	9.894	54.961
5	1.578	5.846	67.256	1.578	5.846	67.256	2.227	8.250	63.211
6	1.290	4.777	72.033	1.290	4.777	72.033	2.143	7.938	71.149
7	1.021	3.781	75.814	1.021	3.781	75.814	1.260	4.665	75.814
8	0.863	3.196	79.010						
9	0.818	3.029	82.039						
10	0.773	2.862	84.901						
11	0.717	2.656	87.557						
12	0.539	1.998	89.555						
13	0.492	1.824	91.379						
14	0.403	1.494	92.873						
15	0.391	1.448	94.321						
16	0.341	1.262	95.583						
17	0.249	0.923	96.506						
18	0.221	0.820	97.326						
19	0.162	0.599	97.925						
20	0.130	0.480	98.405						
21	0.123	0.457	98.862						
22	0.103	0.380	99.242						
23	0.085	0.315	99.557						
24	0.069	0.254	99.811						
25	0.033	0.121	99.932						
26	0.013	0.047	99.979						
27	0.006	0.021	100.000						

Extraction Method: Principal Component Analysis.



PAC Scree Plot for View of All Students on Which Subjects a Degree in Digital Forensics and Cyber Security Should Include

APPENDIX D – Student Workshop Statistical Analysis

Component Matrix [a]

	Component						
	1	2	3	4	5	6	7
Linux Forensics	0.718	-0.477					
Internet of Things	0.712	0.314					
Server Infrastructure	0.657					-0.314	-0.371
Ethical Hacking and Countermeasures	0.655		-0.356	-0.383			
Databases	0.647						0.416
Software Engineering/Development	0.644			0.301			
Mobile Forensics	0.641	-0.582					
Mac Forensics	0.625	-0.511					
Networks	0.597		-0.509				
Computational Mathematics	0.593	0.538					
Project Management	0.543	0.362	0.434	0.301			
Operating, File and Computer Systems	0.534	0.486			0.390	0.314	
Employability Skills	0.515	0.324	0.363	0.330			
Cryptography	0.493				-0.314		
Fundamentals of Computing	0.367	0.704					
Live Data Forensics	0.586	-0.616					
Digital Forensics Tools (Open Source)	0.306	-0.578			0.512		
Digital Forensics Tools (Proprietary)	0.538	-0.569					-0.313
Linux as an Investigative Tool	0.470	-0.547					
Information Security and Assurance	0.397		-0.692	-0.308			
Court Room Skills		-0.314	0.600		-0.360		
Pen Testing Techniques and Tools	0.412		-0.522		-0.371	0.302	
Legal, Professional and Ethical Issues	0.372		0.373	-0.668			
Policing and Criminal Justice	0.524		0.441	-0.573			
Scripting/Programming	0.453			0.463	-0.417		
Contemporary Issues/Emerging Technologies	0.480	0.413				0.551	
Basic Forensic Procedures					0.522		0.568

Extraction Method: Principal Component Analysis.
a. 7 components extracted.

Rotated Component Matrix [a]

	Component			
	1	2	3	4
Live Data Forensics	0.865			
Mobile Forensics	0.836			
Digital Forensics Tools (Proprietary)	0.822			
Digital Forensics Tools (Open Source)	0.749			-0.330
Linux Forensics	0.744			0.305
Linux as an Investigative Tool	0.724			
Mac Forensics	0.684			0.415
Project Management		0.827		
Computational Mathematics		0.758		
Software Engineering/Development		0.626	0.322	
Fundamentals of Computing		0.621		
Internet of Things		0.589		
Cryptography		0.416		0.338

Networks		0.321	0.847	
Information Security and Assurance			0.834	
Ethical Hacking and Countermeasures	0.337		0.661	
Databases		0.345	0.617	
Server Infrastructure	0.415	0.434	0.567	
Policing and Criminal Justice				0.846
Legal, Professional and Ethical Issues				0.803
Court Room Skills	0.325		-0.372	0.570
Contemporary Issues/Emerging Technologies				
Operating, File and Computer Systems		0.363	0.338	
Scripting/Programming		0.303		
Pen Testing Techniques and Tools			0.344	
Employability Skills		0.449		
Basic Forensic Procedures				

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.[a] a. Rotation converged in 10 iterations.

Component Transformation Matrix

Component	1	2	3	4	5	6	7
1	0.565	0.495	0.414	0.312	0.288	0.275	0.089
2	-0.778	0.468	0.174	0.009	0.371	0.090	0.022
3	0.031	0.293	-0.736	0.549	0.074	-0.222	0.121
4	0.145	0.314	-0.460	-0.638	0.015	0.481	0.172
5	0.156	0.100	0.091	-0.371	0.310	-0.700	0.483
6	0.042	-0.541	-0.161	0.059	0.787	0.236	0.012
7	-0.164	-0.220	0.101	0.230	-0.242	0.300	0.845

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

D.4 Views of the Computing Students in a Workshop

In total there were four students in one workshop who identified as studying a Computing degree. All four were male students between the age ranges 18 and 44. Two students stated they had worked in the IT sector before and all prefer an active and practical approach to learning. Each student identified that it was either an interest in Computer Science or IT that was their main reason for choosing a computing degree. One student vocalised this by stating "I chose to do computing because it's where industry is and will be in the future". Two of the students identified they would be looking for a career in private industry, one in the public sector and the other was unsure, roles included software engineer.

When asked if they felt the public are fully aware of what a digital forensics/cyber security practitioner's role is, one student said no and the other expressed they were unsure. Three of the four students expressed that they personally felt the main role and responsibilities of such practitioners are "keeping up to date with technology and techniques", "to be up to date with the latest found loop holes and have ways of tracing or sealing these loop holes to ensure that the risk is minimised or that the culprit is discovered" and "someone that figures out faults in network security and fixes them before an attack can be carried out". These are all valid explanations for a cyber security professional.

The four students expressed that education, training and experience were all important for practitioners in these fields of interest Figure D.4.1. Each noted some skills-shortages they felt of the current industry which included, social skills, "all computer based skills" and more specifically "data analysts [and] security consultants/analysts".

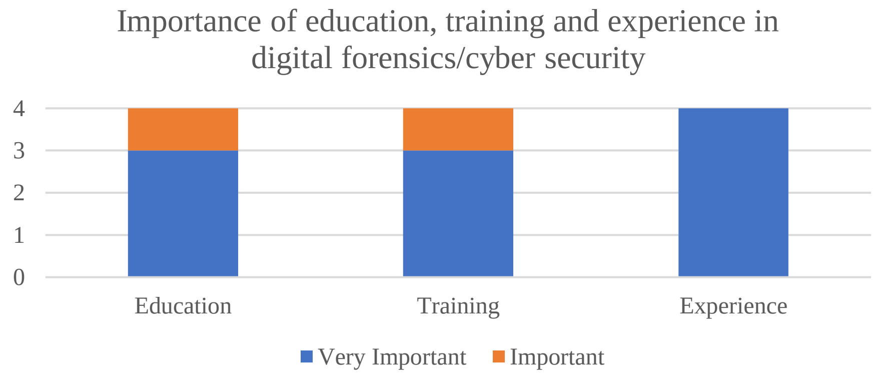


Figure D.4.1 – Importance of education, training and experience in digital forensics and cyber security: the view of a few computing students

Furthermore, all four computing students stated that both theory and soft skills are important in digital forensics and cyber security. One computing student expressed that without theory you are working on the subject from a blind perspective, while other views included the need to understand the risks in using modern technology and protection for Network and computing as the future. One student epitomises the effect of humans in the role of technology stating that “no matter how advanced a security system is human error pose the biggest risk to security. With more fundamental knowledge of security this risk will be reduced.”

When asked what stood out from one graduate to another the students highlighted the responding theme that has been present through this thesis: experience. One student particularly identifies that it does not matter what class of computing degree you obtain, they feel these people would stand out from someone who has a degree in a subject of humanities. Another speaks more specifically about the need to show your ability to execute a specific job or problem and the way one solves these.

What is interesting to see is that the four computing students noted similar qualities when asked what their expectations were of HE and their course prior to starting. Each of the four stated elements of hard-working nature e.g., “more intelligent”, “lots of work, but interesting and relevant to today's industries”, “to gain a better understanding of technology” and “expectations that it would be hard”.

Although these four students interests lie in general computing, they were still able to offer opinions of what they understood digital forensics and cyber security were before starting. One student noted that “as a computing student forensics and cyber security isn't where [their] interests lie but having taken a module on them [they felt it was] an eye opener to their importance”. When asked if their expectations were realistic and met by the course so far, three stated yes with another sure. When asked how their expectations could be met further one student identifies that the ability to “tak[e] the time to research out of education areas [they] find [they] don't understand” would be useful.

This point is particularly intriguing as much of the time spent at university includes students self-learning a vast range of topics and skills outside of their contact time. This may suggest that students may need more guidance on priority interests and topics they are to research more closely. Another identified the need for a “more practical application”, while a third stated that there was a need to “have the security module lectures match the assessment more closely." These points are interesting and offer an insight into how different students view module content and higher education.

Intriguingly, these four students felt that several subjects presented were important and should be included in a degree in digital forensics and cyber security. Of the 27 topics presented, there were four topics which one or more of the four computing students felt were not important at all. These included employability skills, pen testing techniques and tools, policing and criminal justice and court rooms skills Figure D.4.2.

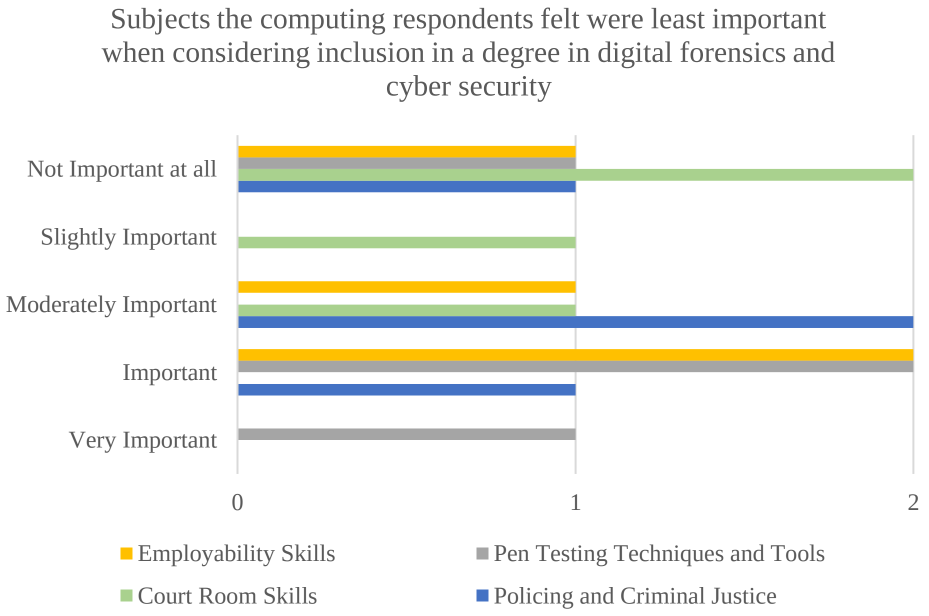


Figure D.4.2 – Computing respondents view on several topics thought to be least important for inclusion in a digital forensics and cyber security degree

All four students, however, rated ethical hacking and countermeasures as very important, along with project management. 16 of the topics or skills were rated by the four computing students as 'very important' or 'important'. The other five topics were rated variously between 'slightly important' and 'very important', as depicted in Figure D.4.3.

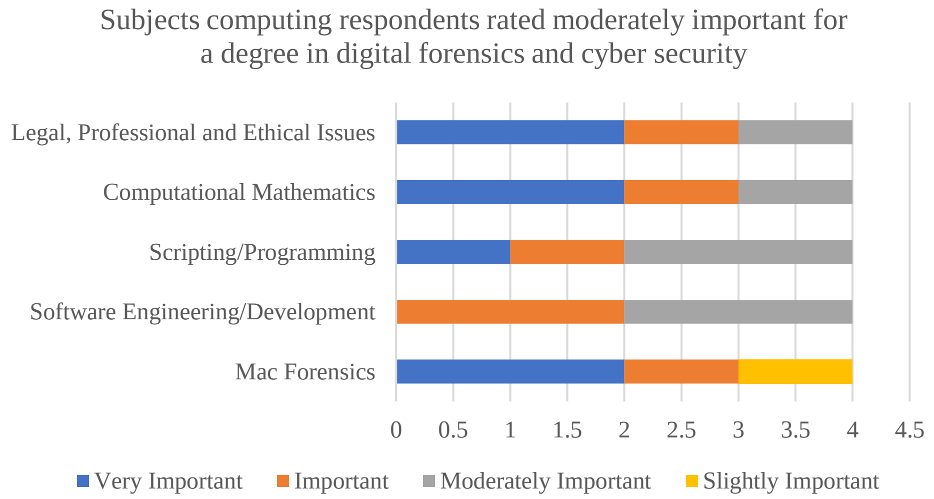


Figure D.4.3 – Computing respondents view on several topics thought to be moderately important for inclusion in a digital forensics and cyber security degree

Final questions for these students included whether there were any further topics they would consider, what they expect or consider is needed to support their future employability on their course and any final remarks. One student responded with “communication skills” as a topic/skill to consider within degree programmes.

Both sociability and communication skills have been mentioned (in these computing student responses) and draw to attention the stereotypical belief that computing students are introvert, ‘nerdy’ and lack skills in social situations. E.g. they are often represented as people who prefer solitary intellectual interests and who are anxious toward interpersonal interactions. However, studies have suggested that there may in fact be an “overrepresentation of Introverts found [particularly] in the programming area” (Greathead, 2008, p. 10). Describing that introverts may be drawn to the discipline through applied skills and enjoyment rather than their potential to lack sociability (Greathead, 2008, p. 10).

This can also be linked to the skillsets of a cyber security professional, where characteristics of an introvert are emphasised by Buchler *et al.* (2018, p. 115) may help when it comes to cyber security in tackling the weakest link: humans (where they are both the problem and solution). Buchler *et al.* (2018) also epitomise the point that maintaining coherence, management and coordination to effectively tackle cyber threats is paramount:

> “Managing the challenges of cybersecurity requires considerable interaction among teams of cyber analysts to monitor, report, and safeguard critical information technology around the 24-hour clock with shift-handoffs.” (Buchler *et al.*, 2018, p. 116)

In previous years, governmental departments including those in the United States have described cross-departmental “understanding of each other’s responsibilities and operational and investigative capabilities as needed to effectively coordinate and collaborate to fulfil … [the] cyber mission” as poor and often “led to conflicts regarding assignments and response to incidents (Office of Inspector General, 2015, p. 6). Therefore, it may be reasoned that a solitary approach to computing, digital forensics and cyber security is poor for achieving the best end results, although the attributes and personal traits which exist in solitary individuals may be good for tackling these largely technical tasks.

In fact, nowadays the need for sociability and communication skills in order to fulfil tasks in computing are seen on a daily basis, where the idea of solitary employees in computing roles is gradually being tackled (e.g. teams of programmers to accomplish a task through problem solving). Therefore, education should include content and assessments which target sociability, solitary, communication, management, and project work to tackle some of these shortfalls.

When responding to improvements, a student stated more focus on student wellbeing was required, while another felt they did not expect anything in relation to employability until their third year of study. This student also highlighted a much bigger concern of theirs in relation to particularly ethical issues. Although a computing student and not studying digital forensics or cyber security, they felt that:

> “Accountability should be taught as ethics. Facebook and Apple for example should not be allowed to do some of the things they are doing without accountability. Also, the materials and labour used to make modern day IOT devices. Students should be made aware of the destruction Apple have done in dredging Tin and their complete disregard to paying taxes. Make the students of the future more aware and morally obliged not to be indifferent on such matters. Perhaps

> encourage students to develop newer materials and technologies that aren't so harmful."

This comment seems more so a rant about companies and the morality behind the processes each undertake, however, the student does have a valid point in their instruction that accountability should be taught as part of ethical considerations in a digital forensics and/or cyber security degree. Accountability is a large part of such practitioners' daily work and businesses alike. For example, a digital forensic analyst must adhere to Principle 3 of the Good Practice Guide for Digital Evidence (ACPO, 2012) which states that "An audit trail or other record of all processes applied to digital evidence should be created and preserved.". While, for example, a business or agency providing digital evidence for the courts must show how the digital forensic lab is accredited, and able to show that they adhere to operational standards: ISO 17025. The standards cover forensic data acquisition, imaging and extraction from hard disk, mobile devices, and removable media as well as analysis of the data found. Accreditation is believed to show that the laboratories conducting such examinations have robust processes, systems, and competent staff: a form of accountability and assurance.

APPENDIX E – PUBLIC PARTICIPANT ANALYSIS OF RESPONSES

This appendix provides chosen graphs which demonstrate responses to a public survey conducted in chapter 10 of 102 participants.

E.1 Gender and Age

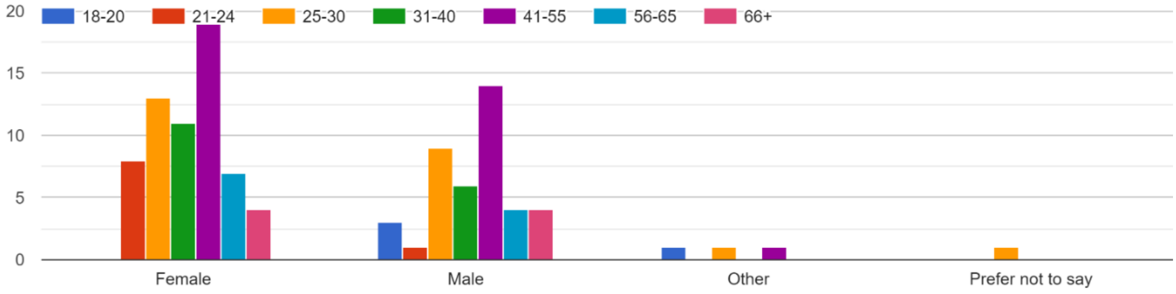


Figure E.1.1 Public Participant Age and Gender

E.2 Employment and Education

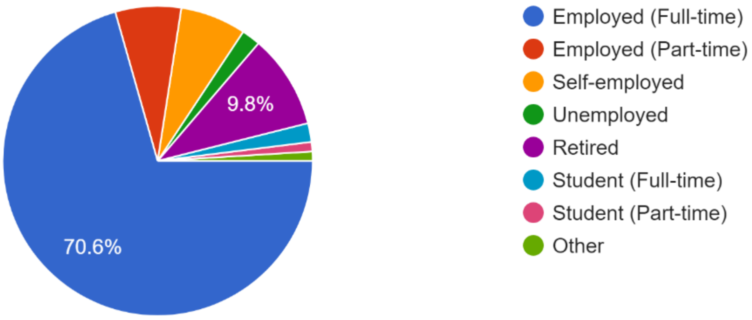


Figure E.2.2 Public Participant Current Employment Status

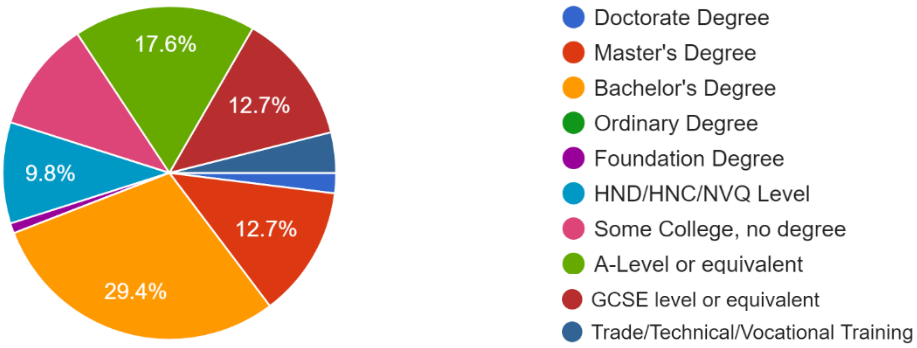


Figure E.2.3 Public Participant Highest Level of Education Completed

E.3 Devices and Activities

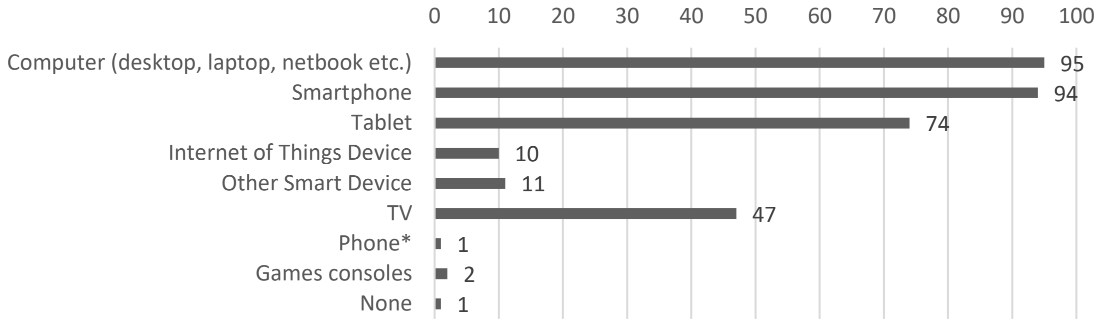


Figure E.3.4 Public Participant Device Usage

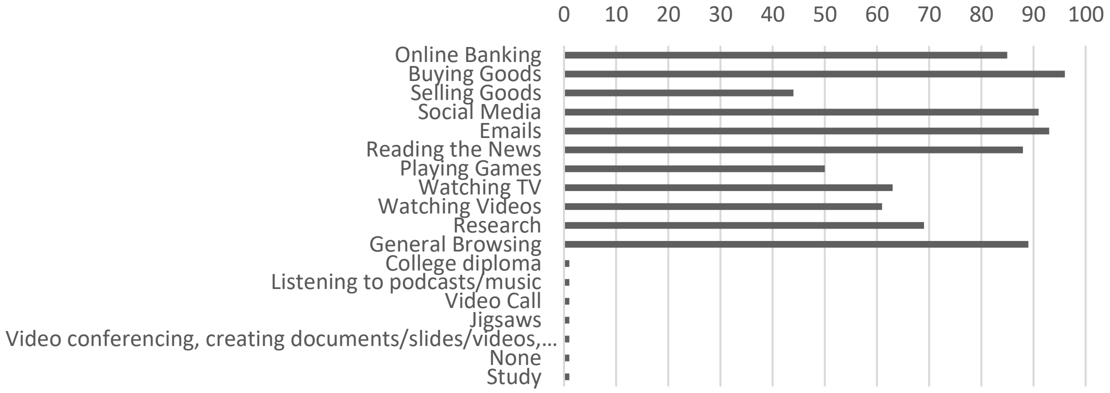


Figure E.3.5 Public Participant Online Activities

E.4 Familiarity with known terms

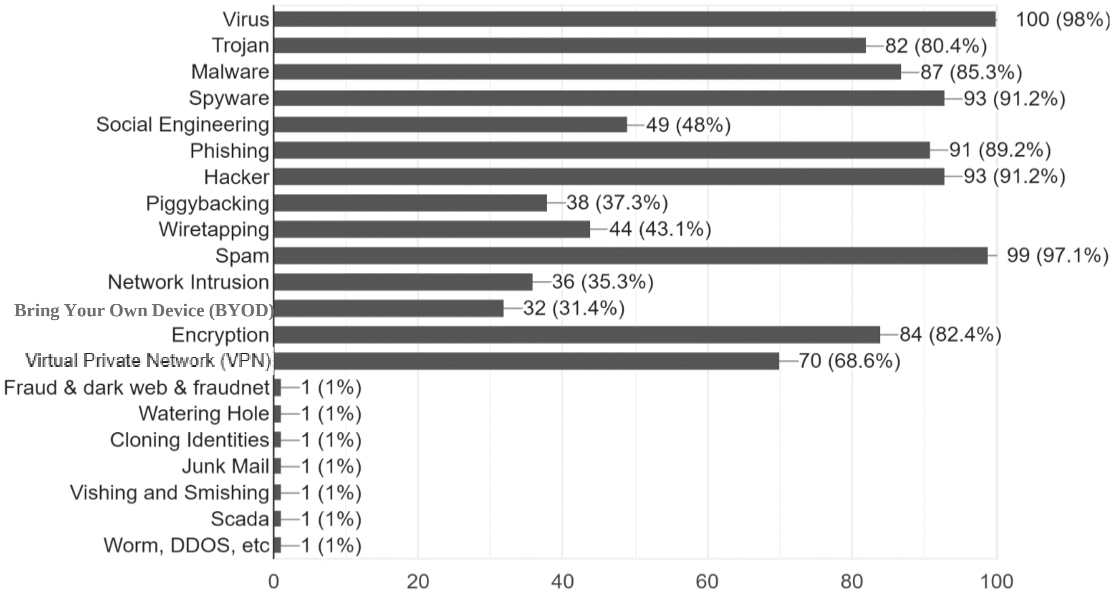


Figure E.4.6 Public Participant Known Key Terms

E.5 Victims of Crime

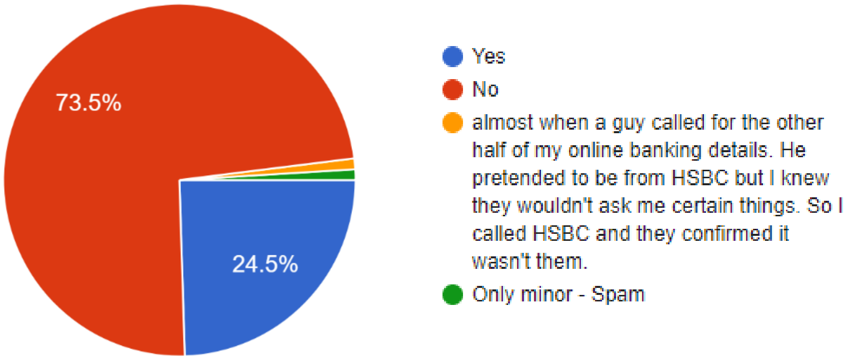


Figure E.5.7 Public Participants as Victims of a Crime

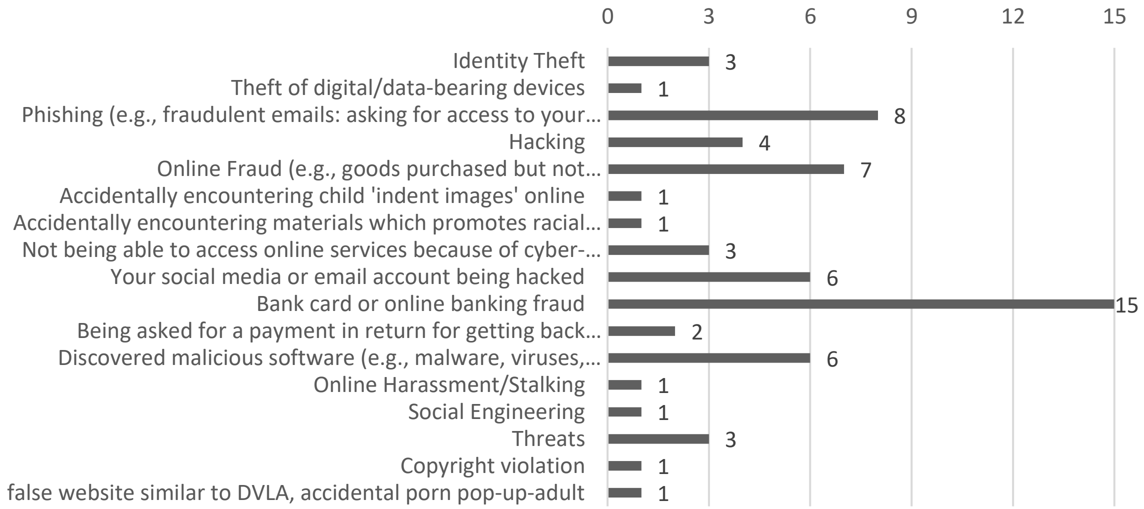


Figure E.5.8 Public Participants as Victims of a Crime: What Crimes?

E.6 Thoughts of Participants of the Terms: Digital Forensics and Cyber Security

This section includes two tables which highlight responses captured of participants on their views of what digital forensics and cyber security are.

E.6.1 Digital Forensic Responses

Examination of all things digital

Analysing data structures and logs from devices to pick up clues about things
Something that the police might do to examine illegal digital activity
Computer security
I think of cleaning up your digital footprint like clearing cookies, ensuring your passwords are strong and looking at your Digital life in forensic detail to ensure that it is secure.
Analysing digital use
Robots dusting a crime scene for finger prints
Computer forensics
NCIS and McGee
Tracing the culprits
Taking apart a computer for examination
Investigation & recording of digital crimes
Police related cyber crime
Investigating Internet crime
The investigation into cybercrime & digital activity
Analysis of digital and electronic devices
Investigation on materials of digital devices
Describes the ability to analyze data left or held on a device like a digital footprint in the same way a crime scene investigator can review a crime
American TV series
Obtaining evidence of activities from (any type of) computing devices
Reviewing the digital footprint left behind by any interaction between a person and a digital device bot online and off.
Tracking online activity
High level investigation of a digital environment
Makes me think of a TV crime drama like Broadchurch or The Killing - but rather than being at a murder the detective is probably in an office or home computer.
Identifying digital footprints on a device
Do not understanding
Someone who investigates electronic crime.
Following internet trails
Data investigation
The ability to investigate and recover different materials found on different digital devices especially in relation to crimes
Used in terms of checking coding re: malware, or following the digital trail of an online fraudster or hacker...etc. Or using digital devices to access, investigate, monitor, or recover information relating to a crime.
Crime evidence found on electronic devices.
Use of technology to enhance current forensic techniques, as well as being able to use transitional forensic techniques to transpose into the digital world.
Someone who investigates online and computer crimes (hacking, etc.)
Unsure
Looking back on computers to find any wrongdoings
Data recovery and analysis
Investigating paedophiles, hacking and fraud?
Finding traces of what caused the problem either the trail after a virus or the malware lurking on a system

The digital equivalent to traditional forensics, investigating the digital 'footprints' left by perpetrators of crime.
Police investigation to online crime.... hacking, tracing online activities etc... NCIS CYBER
Similar to computer forensics, but based on digital content rather than hardware?
I hope the crimes are being watched
Forensic examination of digital data.
Investigating cyber crime
Detectives of the internet world
Forensics on digital devices
I do not know enough about it
All forms of criminal based investigation into digital devices incl. those used to commit or facilitate crime and those that provide passive data. Includes devices and internet / data storage
Tracking a trail of clues left by digital naughtiness.
The science of studying digital information and the systems through which it is relayed and coded (this is a guess)
Recovering information in relation to computer crime
-
Investigation to get to the root cause of an issue
Recovering information that are on devices involved in crimes.
Investigating people’s digital offences
Inspection of digital footprint left on computers hard drive
COMPUTER CRIME
Not sure
The checking of people’s personal usage of the internet/searches/social media etc.
No idea
The ability to decode encrypted data. The ability to trace activity with specific data.
Scientific research
Investigating Cyber crimes
Forensic science within digital services
Investigating digital crime
Investigating cyber security and devising methods of preventing it
Researching into digital activities
Computer police
Investigation
Analysis of data in a forensic capacity, with a view to establish a truthful timeline of events or to recover lost data.
Use incognito browser & Hide my laptop
Banking
A man (and it is a man) analysing an attack to find out where it came from, block it for further attack and if possible pass information on for conviction
Analysing the total memory and usage of a digital device and any programs associate to it.
An area of science that researches what/where an electronic device has been used and what it has been used for and who by.

Data analysis and recovery for a formal procedure
Deep examination of storage where possible direct to the hardware
Investigations into the origin and extent of online wrongdoings.
Cyber crime
Recovery and investigation of material found in digital devices
Gathering evidence surrounding a cyber intrusion/attack/crime
Analysis of data in order to assist with an investigation
Investigation of digital data usually because of crime
Searching through digital crime scene to find out what happened.
An investigation in the digital world.
Crime
Forensics
Using digital methods to detect origins of cyber crime
Investigation and discovery of evidence of cyber crime
Investigating things on a computer
Investigations into online crime
The process of finding or retrieving digital information from devices
Analysing data
Police looking for internet criminals.
Investigating online activity
Police investigation of cyber crime
Forensics in a digital context
Uncovering and interpreting digital data
Looking for answers and or evidence of how or why a digital crime has happened

E.6.2 Cyber Security Responses

Online security
Protection of online info
Anti-virus
Minimising potential threats from physical and network sources
Protecting yourself or your company from potential attacks
Cyber Security?
Anti-Virus, robust passwords, private & secure networks
Being secure online
A robot standing at the door of a club waiting to check people's ID's
HTTPS and links. Looking for fraud (including spelling etc. and spam). Email addresses. Asking for bank account details.
Trying to stop the culprits
Security involving computers/phones/other smart devices over the Internet
Online security. Anti-viruses
Protection and virus scanners
Web protection
Protection for your data used online

Protection and securing of electronic devices
Protection of cybercrimes on devices
A topic cover ways to protect yourself on digital devices to avoid social engineering or hacking.
The Bank
Protecting digital assets from unintended access, modification or denial of their use
Keeping personal information secure when accessing a digital pathway.
Online steps taken to secure information
Security related to digital environments
A list of help or advice to keep you safe online? A protocol?
Protection from online attacks
Do not understanding
Passwords, personal details
Protecting data/software etc
Computer security
It is the protection of a computer system or digital device from damage or theft of its software or data and stopping any disruption of any services they may be providing.
Firewalls, anti-virus, anti-malware... etc.
Computer and online security.
Protection methods for use of technology.
I assume it is securing oneself from potential hackers who could gain private data or being robbed of money.
Keeping safe online
Stopping computers etc from being hacked and infiltrated.
OS, application and network security
Trying to stop my devices being compromised
Keeping the digital safe from crime
Any security aspects relating to your digital life, such as password policies, antivirus protection, firewalls, maintaining control over personal information, etc.
As above but the protection and prevention side
The prevention of, attacks and or unauthorised access to a networks, data and machines (severs, PCs etc.)
I think of software
Password protected and anti-hacking
Protection for data kept or used on the internet
Policing of the internet world
Security against attacks on digital devices
Preventing access to data and digital devices or storage, networks
Computer protector
Firewall, pc safety, protecting one's devices from viruses and/or hacking. Also, larger organisations collecting data for their own protection.
Protection of data
-
Protecting online data
Security on the web

Companies you pay and check what you are doing on the internet is safe
Firewall and other systems which prevent computer hacking
COMPUTER PROTECTION
Help with security online
The protection of one’s personal data.
Protecting yourself online
Network security, firewalls, DDoS'ing.
Putting measures in place to prevent cyber crime
A body designed to secure and protect computer-based systems
Security surrounding anything deemed 'online'
Securing internet connections to prevent breaches
Protecting and safe guarding
Internet security
Safety, prevention, security, hackers, identity theft
Anti-Virus, Firewalls and other similar technologies.
My laptop isn’t up to scratch
Prevention of attacks
Virus checkers and fire walls
Either an individual or an organisation taking measures to ensure that their information is secure when using electronic devices or communication. As simple as thinking of what you put on social media to multi million investment in to digital security.
The protect of a system from intrusion
Buzzwords that few understand in any practical sense
Protection against online intrusion
Complicated
Hacking
Steps taken to protect and environment from cyber crime
Security that is put in place to protect your data on a computer or smart device
Prevention of data being accessed by someone who should not have that data
Any digital security, laptops, tablets, android, iOS anything digital.
Digital security
Don't know
Internet fraud
Defensive mechanisms to avoid being attacked - firewalls, VPN etc
Keeping safe the internet and devices used
Staying safe using digital devices
Protection against crime for any device able to access online content
The practice of protecting infrastructure from the risks of online viruses / hackers
Firewall's passwords secure networks
Not sure
Protecting online activity
Antivirus systems/software and updates
Worry
Protection of computer systems from theft or damage of hardware, software and information

Prevention of cyber intrusion
Protection of my online devices

E.7 Thoughts of Participants on What Should be Tacked in Society

Respect for others feelings and belongings
General ignorance
Everything above! I think digital crime is only going to get worse and at the moment, the police are perhaps a little ill-equipped to deal with this.
General education about staying 'safe' online.
2 factor authentication should be compulsory for all sites requiring sensitive info, voice recognition should be compulsory as part of this, cyber bullies should be able to be barred from the internet for all uses.....that would be a good punishment as a min up to and including jail time
Stricter monitoring or access to sites
Identity theft and fraud
More security
Fraudsters from outside the UK. Allowing people to setup dodgy sites and spam emails.
Stronger penalties
People need to be more aware of the potential problems and act vigilantly
Better public awareness. Tighter controls online & less anonymity online, not for the average user but for advanced users like those who use the Dark Web.
More visible policing of sites
Hackers and fraudsters
Websites are more secure and harder to hack, it's becoming more common for information to be leaked and personal identities stolen
The image of a forensic analyst. We are not NCIS two keyboard hackers Paul.
More knowledge and how to deal with it if it happens to you.
Harsher punishment of identity thief and the ability for the police to gain access if reasonable proof can be provided
Stop relying on everything digital
Motivations or perpetrators to reduce risk, training and education, certifications in relation to devices
Raising the profile of cyber/digital crime to show it is not victimless. Raising awareness of how to protect yourself from digital and cyber crime. Providing free confidential and reliable advice to victims of cyber crime.
Stronger international cooperation about all of the above
Social awareness and preventative measures
Cyber bullying; trolls on twitter; being kinder
Greater understanding of the threats
Everything
Child-Abuse Money-Banking Terrorism
Awareness, making sure everyone knows the risks and how to protect themselves
Being taught at schools about cyber security, involving younger generations in digital crime prevention.

I think that people need to be made aware of the different types of cybercrime that are prevalent in society at the moment and the simple tasks they can use to prevent themselves becoming a victim
Education and awareness are a must and should be easier/cheaper to access to everyone. Understanding is key.
Hacking of online transactions, shopping and banking.
Understanding. Too few still understand what a spam email is. I education is key to prevent the increase of digital crime
More awareness
Unsure
People need a better understanding of how they can be scammed.
More efforts should be put into education regarding general Internet hygiene, phishing, viruses and the dangers associated with these to help in prevention
Same as off line crime, people need to learn respect for others and themselves, so they don't commit crimes. Tall order I know!
Educating others as to the impact of a little anonymity on how people react - look at trolling! Also, lots of issues surrounding people not knowing the expectations or rules online - hacker is not a dirty word.
People need to acknowledge that it's truly wonderful to live in this interconnected world, but that your private data is as precious as your life and that fairly minimal precautions can ensure a reasonable degree of protection.
Not sure
Making people in general aware as to how easy it is to gain information on them. How liberally people use the internet without realising they could be passing on their information unwillingly.
Awareness
More awareness of bullying via social media such as trolls
The apparent belief that the anonymity of the internet excuses bad, cruel or rude behaviour
Ensuring data protection.
Not sure
.
Education
Better education
More transparency in who has access to what information - so we know what the govt/police etc., take from us & know from us.
Updates in systems to secure prevention.
-
Making people aware how to remain as safe as possible
How people view/use the internet. Security risks are not taken as seriously as they should be.
There is so much freedom for all users on the Internet. I really do not know what can be done.
Raising the profile and educating all levels of users about how to prevent hacking of their computers
SCHOOLS NEED TO TEACH CHILDREN MORE ABOUT IT
Better information for older users
Education at home & in schools. More responsibility placed in the hands of those making millions out of the internet. You Tube Google Bing Facebook, they're very happy to take our money but they don't provide sufficient protection.
Need to pursue hackers more aggressive

This hasn't affected me, though I see a lot of articles in the news recently about teenagers sharing explicit images between them and of course you have paedophile rings that need to be found and dealt with. The digital age has made it far more easy for people to negatively impact people's lives while at the same time being a valuable asset in people's lives. There needs to be an established mid-ground where the internet can be used properly.
Awareness online
Better protection more knowledge of what is occurring and how to prevent
I wouldn't know where to start in answering this
Harassment, impersonation, benefit fraud, child abuse
Websites that should not be visible to children, personal data security
Paedophilia, child sexual exploitation, bullying, hate crime
Child porn
Wider awareness, personal responsibility, better support, businesses that can give domestic IT support and security
Awareness that this is a new and growing problem and the general attitude of those who consider it a lesser crime compared to its physical counterpart.
Updating appropriate legislation, less sweeping powers by the state. Cyber bulling, copyright issues, self-censorship and the 'social cooling' effect, mass education of cyber sec from a young age
Child abuse
I'm not sure, sorry
More awareness and easier access to security software
The biggest problem that I have to deal with is cyber bullying and the fall out that this can have. This may seem insignificant compared to multi million pound cyber crime but if we teach how to look after the simple at a young age and what it is appropriate to share and how to not be duped then these are skills that could be transferred.
Awareness and the ability to prevent it
Education, because 'cyber' is not tangible, people care less about their passwords than house keys.
Education. People are still not aware of what they should be looking out for when trying to spot attacks on them, and are given sometimes conflicting advice about how to protect themselves.
Awareness
Better education made available on how to protect your device and information online
Awareness among general society of the vulnerabilities needs to be improved, and the possible consequences to individuals affected made clearer.
More knowledge on the subject for public so they understand the consequences of some of their actions, when not protecting themselves.
Better understanding of what makes you vulnerable
Education, Education, Education. So many people don’t understand digital crime.
People need to be more aware.... somehow....
Awareness and education of a number of related things.
Financial crime
A general understanding of the technologies and the dangers involved
The actual source of criminal activity
Make people more aware of the issues and how to stay safe
Making users more aware and responsible for the need to have suitable protection in place

A greater understanding by the general public of the risks etc
People need to be more aware themselves when receiving unexpected contact via the Internet
Social Media problems
Making people more aware of the risks and to keep vigilant.
Education of prevention and education of consequences
The perpetrators
Teaching 3 stages of defence: prevention, incidence management, consequence management
All of it

E.8 Password Usage

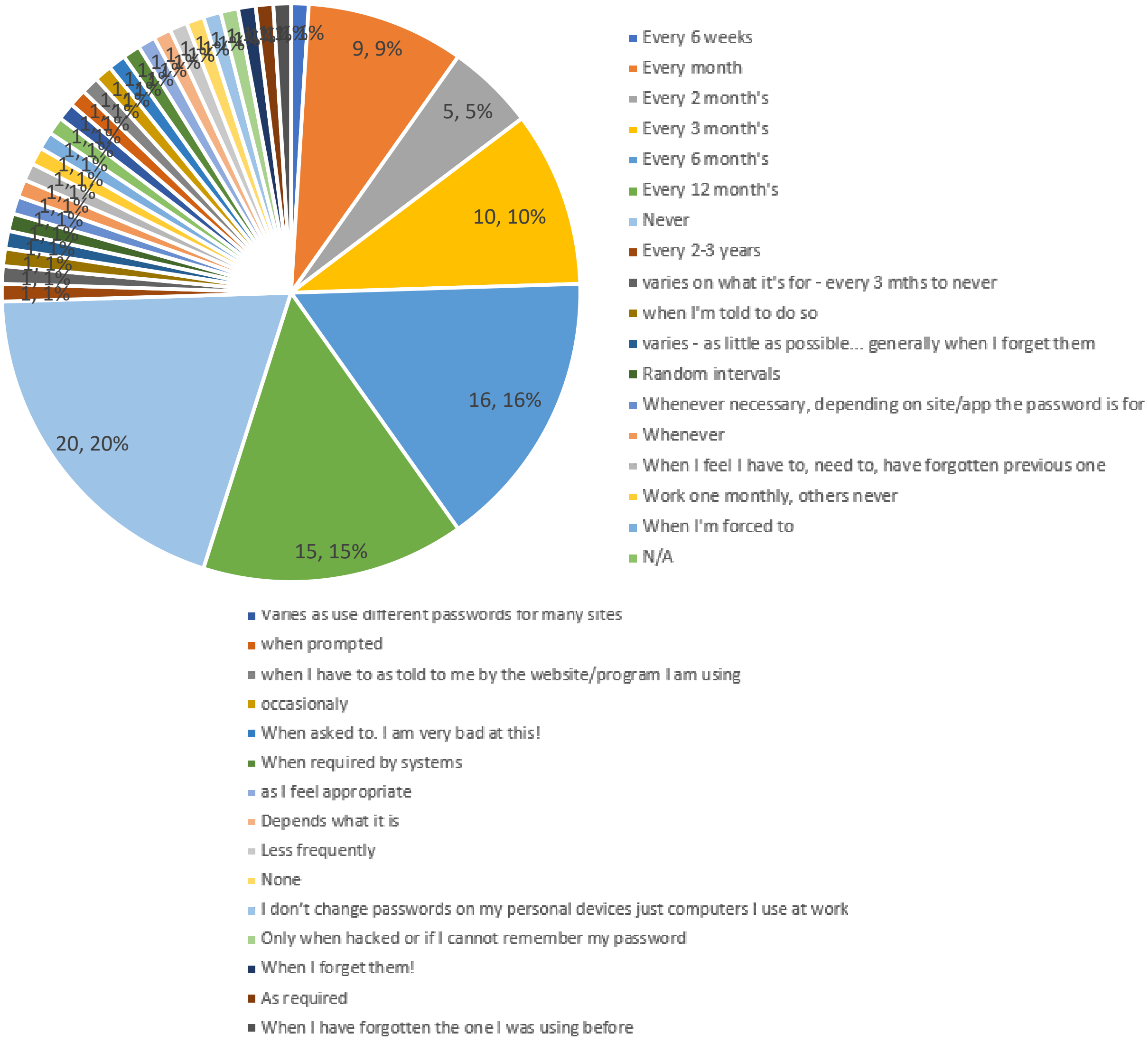


Figure E.8.1 How often Public Participants Change their Passwords

Figure E.8.1 demonstrates the schedule that participants admitted to changing their passwords at home. As the chart shows approximately 20 percent of the 102 participants admit to never changing their passwords. Meanwhile, a further 16 percent admitted it was every 6 months, and a further 15 percent every 12 months. Approximately 10 percent admitted it was every 3 months, 5 percent every 2 months, while 9 percent stated they changed their passwords monthly. All other responses which are discussed in chapter 8 and identify themes such as, when people are told to change their passwords through to only when they cannot remember the password or may have been hacked.

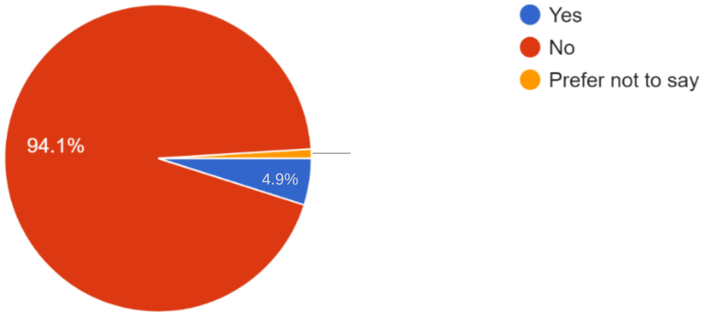
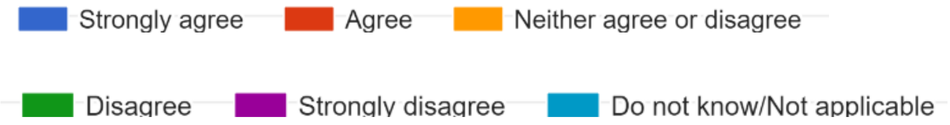


Figure E.8.2 Public Participants use of Examples of Poor Passwords[72]

E.9 Views on Technology, Security and Personal Data: Likert Responses

Below are the key colours for the Likert scale used for the following charts:



[72] Examples included 123456; password; 123456789; qwerty; 123123; google; 111111; qwertyuiop; 1q2w3e4r.

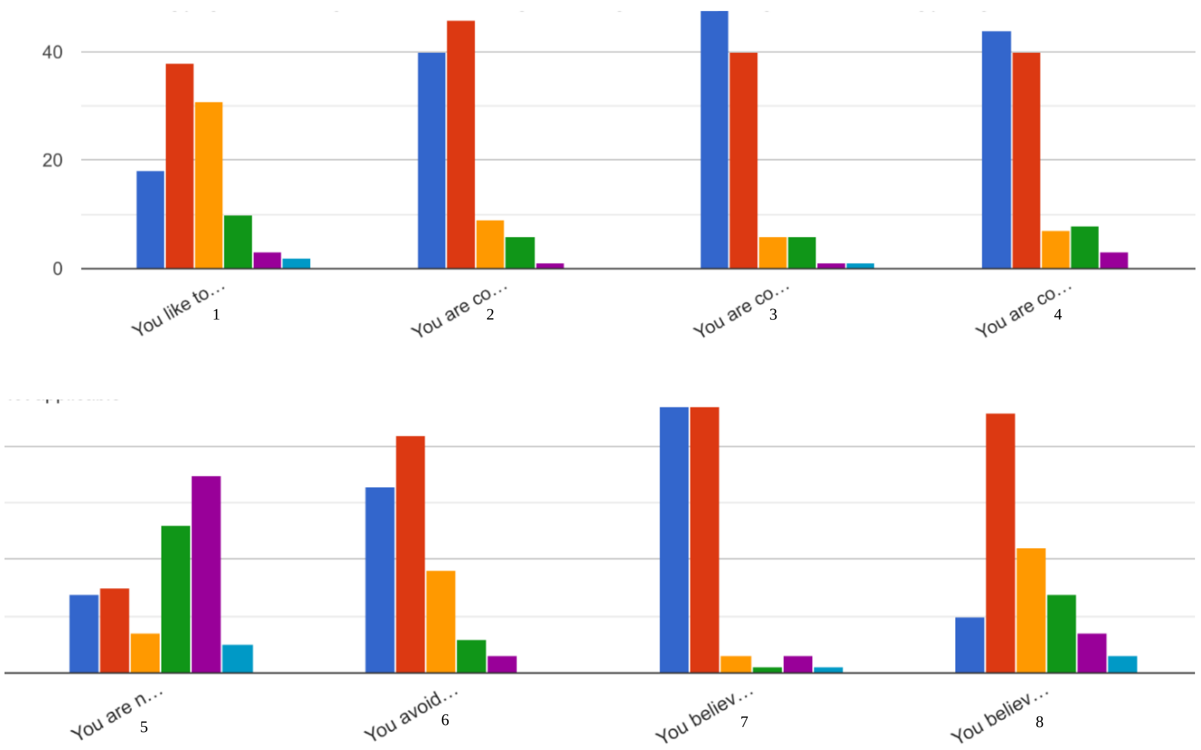


Figure E.9.1 Public Agreement with Statements on Technology, Security and Personal Data[73]

[73] Statements are outlined in section 8.10. Statements consider the following issues: 1. using and tinkering with technology 2. concerns about privacy 3. concerns about security of digital devices 4. concerns about security of personal information by websites 5. concerns about the security of online personal information by public authorities 6. disclosure of personal information 7. risk of becoming a victim of digital/cyber crime 8. protecting against crimes.

APPENDIX F – SUBJECT FRAMEWORK ANALYSIS

This appendix considers the fresh delivery of frameworks within cyber security and digital forensics for academia. Frameworks most pertinent to the discipline have been identified and subjects as well as skills and competences are considered in light of a lack of framework and academic standing within the discipline.

F.1 NCSC - Cyber Security, Computer Science and Digital Forensics Certification of Bachelor’s and Master’s Level UK Higher Education

The UK Government Communications Headquarters (GCHQ)[74] set out to certificate educational programmes involving flavours of cyber security and now digital forensics at both Bachelor’s and Master’s level where certification can take place for eight different types of degree programme (NCSC, 2018b, 2018a). Initially, only four universities were regarded as worthy at offering “an acceptable standard” of education within the general topic of cyber security to receive full certification at Master’s level (Parr, 2014). Since then, several Master’s degree programmes across the UK have been certified (GCHQ, 2016; NCSC, 2018b), either having received full certification or provisional certification[75]. The number of HEIs with full and provisional certification now depicted in Table F.1.1[76], according to NCSC (2018b) where, three are categorised as digital forensics:

NCSC Certification	Full certification	Provisional certification
Master’s degrees	14	11
Integrated Master’s degrees	0	3
Bachelor’s degrees	1[77]	2

Table F.1.1 – NCSC Certified Course Numbers

[74] Now examined under the National Cyber Security Centre (NCSC), a part of GCHQ

[75] Full certification requires a programme to have been running in the current and previous year (certification lasts for five years) and provisional certification the programme need not have started or is running the current year (certification lasts for two years or until the first cohort of students have completed) (NCSC, 2018a)

[76] As of November 2018.

[77] Edinburgh Napier University were the first to receive full certification and include Digital Forensics (Edinburgh Napier University, 2018).

Courses are assessed for certification by a minimum of three representatives across "GCHQ[74], wider government, industry, professional bodies and academia" (NCSC, 2016, p. 9). They are then scored by each member who assesses aspects including: content and materials, research dissertations, assessment, student numbers and descriptions relating to the course, institution and staff (NCSC, 2016, 2017a). Each applicant is required to submit a breakdown of current course entries, student numbers, grades and student satisfaction scores as evidence (NCSC, 2017a, p. 41). While few courses hold full certification, several questions may be raised including but are not limited to:

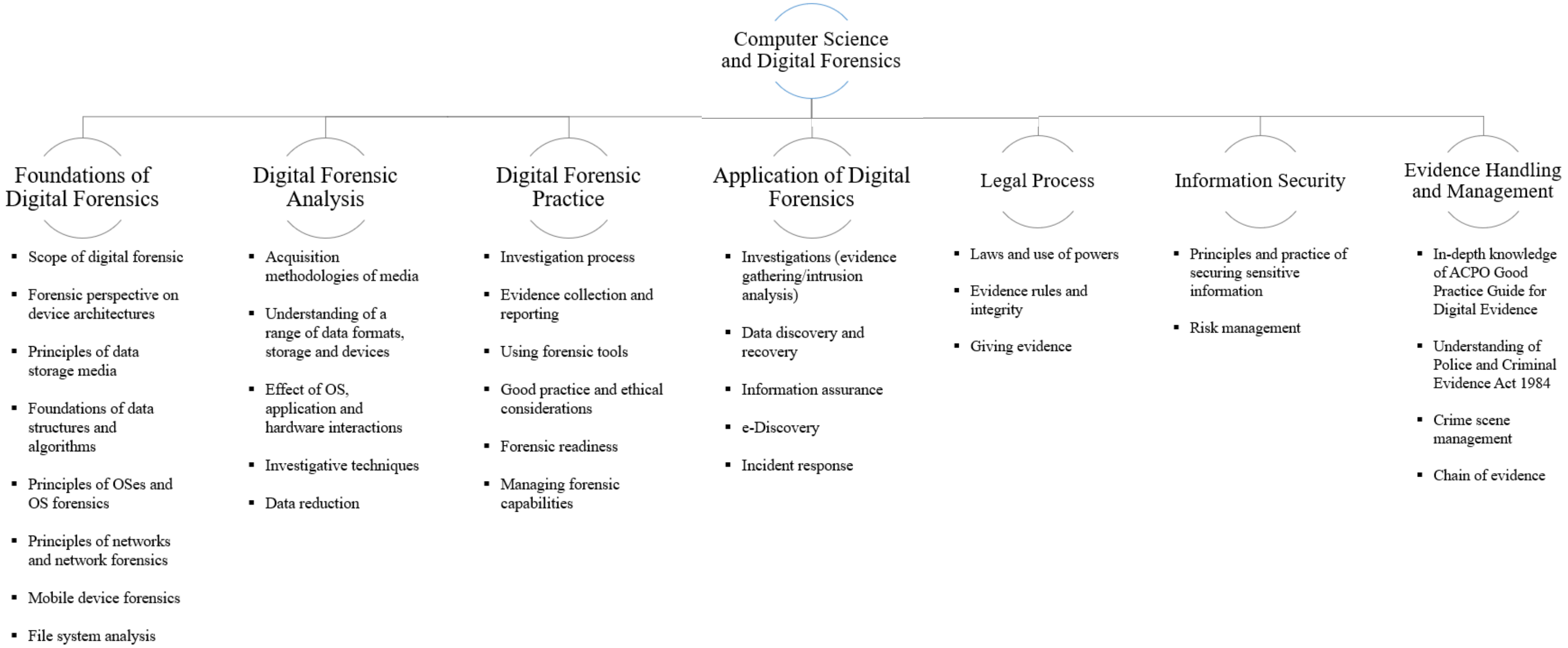
- What are the requirements for certification based on, and how was it comprised (e.g. working partners and courses used as a template)?
- Are the requirements for certification inclusive of all HEIs (e.g. post-92 universities as well as Russel Group universities)?
- What if all programmes within the UK are certified; what is the worth of certification?
- Why are programmes not being certified, or why are HEIs not submitting cases forward to be certified (i.e. how could courses not meet the specification set)?
- What benefits do these certifications bring to a course and what does it add professionally?
- What do the certifications outline for digital forensics curriculum, and how does this relate to other similar frameworks?

A study of the literature cannot answer these questions; however, it can be used to identify topic coverage and comparison to similar frameworks.

The Bachelor's degrees in digital forensics documentation highlights several topics which must be covered on a course (depicted below in Figure F.1.1 and Figure F.1.2). To qualify for Master's level certification the standard states courses must "address[] Digital Forensics in law enforcement and intrusion analysis, with emphasis on law enforcement" (NCSC, 2016, p. 3, 2017a, p. 4). Certification call documentation identifies with "Security Disciplines … and Principles from the IISP[78] Skills Framework" as well as identifying with the "CESG's documentation on the Certification for IA Professionals" (NCSC, 2017a, p. 15). IISP disciplines and principles include those relating to incident

[78] The Institute of Information Security Professionals (IISP)

management, investigation and responses, intrusion detection and analysis and forensics ranging from basic skills in "describ[ing] the basic principles or digital forensics" through to more complex understanding and technical competencies and analysis techniques to lead digital forensics investigations (The Institute of Information Security Professionals, 2018, pp. 22–24). The NCSC framework along with IISP framework have similar comparisons with the 'ACM Cybersecurity Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity' (Joint Task Force on Cybersecurity Education, 2017) and the 'US National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework' (Newhouse *et al.*, 2017).



Computer Science and Digital Forensics

Foundations of Digital Forensics

- Scope of digital forensic
- Forensic perspective on device architectures
- Principles of data storage media
- Foundations of data structures and algorithms
- Principles of OSes and OS forensics
- Principles of networks and network forensics
- Mobile device forensics
- File system analysis

Digital Forensic Analysis

- Acquisition methodologies of media
- Understanding of a range of data formats, storage and devices
- Effect of OS, application and hardware interactions
- Investigative techniques
- Data reduction

Digital Forensic Practice

- Investigation process
- Evidence collection and reporting
- Using forensic tools
- Good practice and ethical considerations
- Forensic readiness
- Managing forensic capabilities

Application of Digital Forensics

- Investigations (evidence gathering/intrusion analysis)
- Data discovery and recovery
- Information assurance
- e-Discovery
- Incident response

Legal Process

- Laws and use of powers
- Evidence rules and integrity
- Giving evidence

Information Security

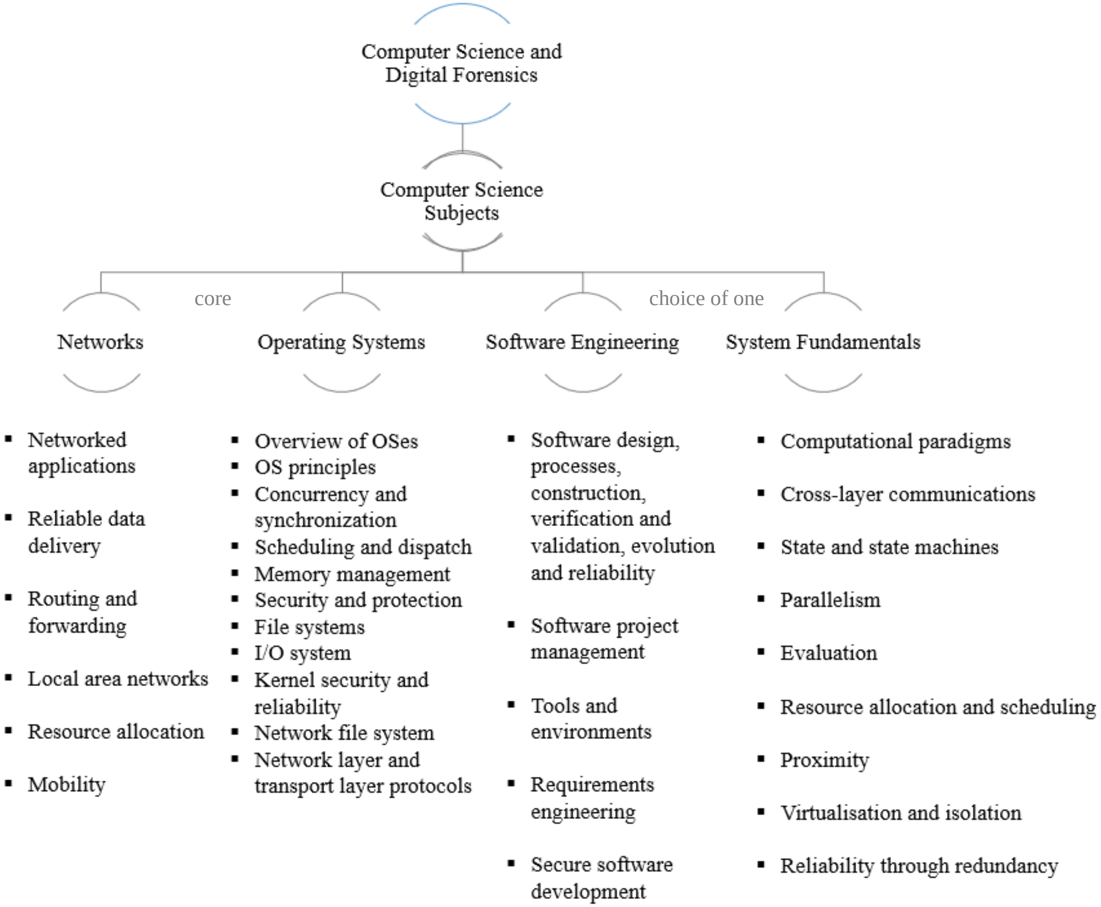
- Principles and practice of securing sensitive information
- Risk management

Evidence Handling and Management

- In-depth knowledge of ACPO Good Practice Guide for Digital Evidence
- Understanding of Police and Criminal Evidence Act 1984
- Crime scene management
- Chain of evidence

— (taken from NCSC, 2017b, pp. 23–24)

Figure F.1.1 – NCSC Bachelor’s Certification Computer Science and Digital Forensics – Digital Forensics Curricula Knowledge Areas


Computer Science and Digital Forensics
Computer Science Subjects
core
choice of one
Networks
Operating Systems
Software Engineering
System Fundamentals
▪ Networked applications
▪ Reliable data delivery
▪ Routing and forwarding
▪ Local area networks
▪ Resource allocation
▪ Mobility
▪ Overview of OSes
▪ OS principles
▪ Concurrency and synchronization
▪ Scheduling and dispatch
▪ Memory management
▪ Security and protection
▪ File systems
▪ I/O system
▪ Kernel security and reliability
▪ Network file system
▪ Network layer and transport layer protocols
▪ Software design, processes, construction, verification and validation, evolution and reliability
▪ Software project management
▪ Tools and environments
▪ Requirements engineering
▪ Secure software development
▪ Computational paradigms
▪ Cross-layer communications
▪ State and state machines
▪ Parallelism
▪ Evaluation
▪ Resource allocation and scheduling
▪ Proximity
▪ Virtualisation and isolation
▪ Reliability through redundancy

— (taken from NCSC, 2017b, pp. 16–17)

Figure F.1.2 – NCSC Bachelor’s Certification Computer Science and Digital Forensics – Computer Science Curricula Knowledge Areas

F.2 ACM - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity – A Joint Task Force Report (2017)

The Joint Task Force report focuses on 'Cybersecurity' curriculum, seeking to develop a "flexible curricula guidance in cybersecurity education" (Joint Task Force on Cybersecurity Education, 2017, p. 10). The idea of the report is to address the need for "proficiency" within the cybersecurity education, providing a module design and guidance for fundamental topics, content and practices. Though the framework addresses cyber security education, the underlying and central comprehension identifies that there are several key topics which should be inclusive in such a technically heavy and specialist educational course.

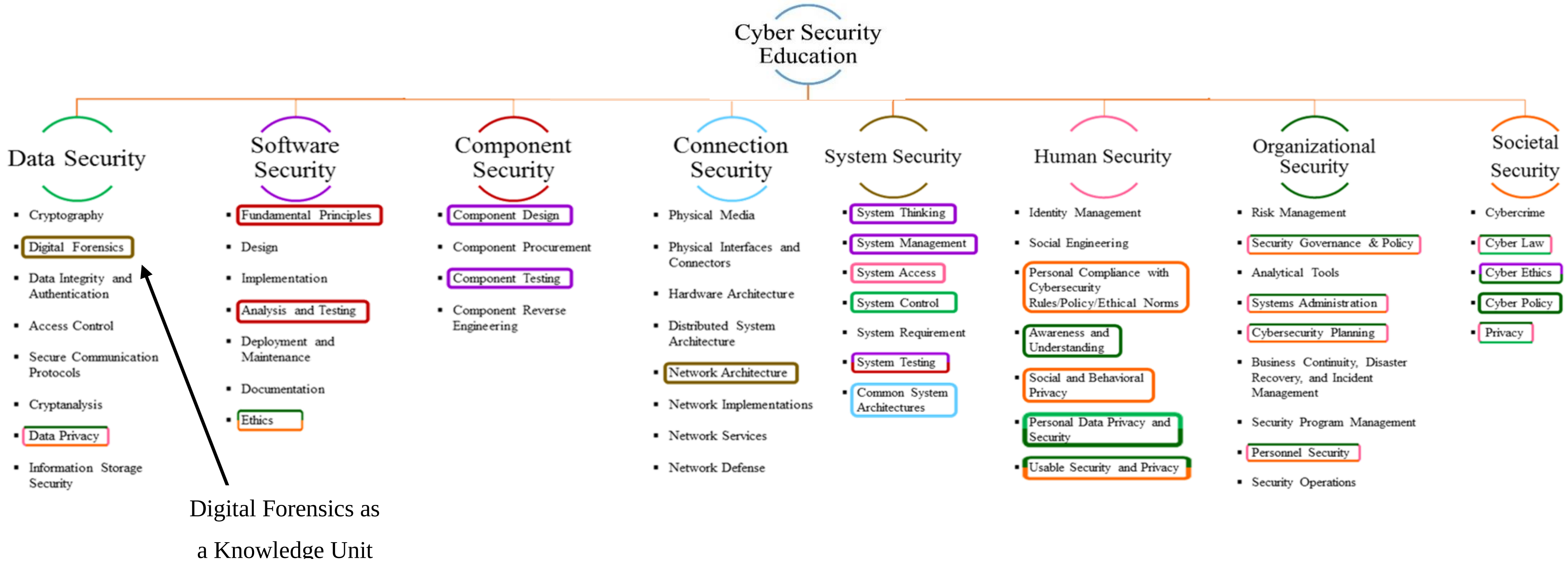
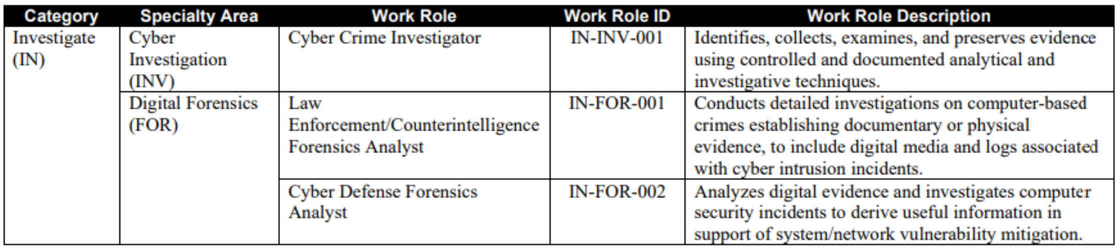


Figure F.2.1 – ACM Cybersecurity Curricula 2017 Framework Knowledge Areas

F.3 NICE - US National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

The NICE initiative is a conceptual framework established by a community of subject and academic experts which extends into much lower level details of what is expected of cyber security and digital forensics professionals. As documented in Figure 3.3 in chapter 3, the framework divides categories into specialist areas and professional roles. Each role is described and broken down by Knowledge, Skills and Abilities (KSAs) and tasks which are expected of each professional (Newhouse *et al.*, 2017, p. 6). Within the framework there are three roles which relate to investigations, two of which are categorised as digital forensics, depicted in Figure F.3.1 (Newhouse *et al.*, 2017, p. 23).



Category	Specialty Area	Work Role	Work Role ID	Work Role Description
Investigate (IN)	Cyber Investigation (INV)	Cyber Crime Investigator	IN-INV-001	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.
	Digital Forensics (FOR)	Law Enforcement/Counterintelligence Forensics Analyst	IN-FOR-001	Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.
		Cyber Defense Forensics Analyst	IN-FOR-002	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

— (taken from Newhouse *et al.*, 2017, p. 23)

Figure F.3.1 – Three roles relating to digital forensics in the NICE Cybersecurity Education framework

Looking at the two roles categorised under the speciality ‘Digital Forensics’ there were common KSAs and tasks found of both roles. Table F.3.1 (below) depicts these common attributes in effort to highlight what ideally may produce an effective digital forensic professional.

The knowledge, skills, abilities and tasks show that fundamentally digital forensic practitioners should be expected to have an in-depth and broad understanding of the inner workings of digital devices. They also stress that students must gain knowledge, and understand of relevant legislation, guidelines and procedures which relate to digital evidence. Furthermore, this includes the investigative processes behind collecting and preserving, handling and transporting evidence, storing and analysing evidence and chain of custody. Procedures within this documentation are US-based, however, these may be national or cross-jurisdictional in nature.

Knowledge also includes physical attributes (e.g., what components can be found in a computer and what they do) as well an understanding of what happens on a range of operating/file systems and where particular files maybe be found and analysed which may provide vital evidence. This list suggests that digital forensics and cyber security work hand-in-hand with one another, a debate which is discussed further in chapter 3, where practitioners should be expected to have gained knowledge of cyber security aspects such as, principles and privacy, application and system vulnerabilities, risks and risk management, information security and hacking methodologies.

Interestingly the framework identifies the use of specific forensic tools as a skillset of such a practitioner; examples of tools mentioned include proprietary and open source tools. This is different from the works of the NCSC and Joint Task Force who mention digital forensic tools as a topic, however, prevent from naming suites they consider should be covered. While, the Joint Task Force on Cybersecurity Education (2017, p. 26) do mention the necessity to know the requirements of different types of tools as well as their limitations, and examples such as, "Artifact-focused versus all-in-one tools".

Knowledge Skill Ability or Task	**Explanation**[79]
Knowledge	"physical computer components and architectures including functions of components and peripherals"
	"types of digital forensics data and how to recognise them"
	"system files which contain relevant information and where to find them"
	"file system implementations"
	"computer networking concepts and protocols and network security architectures and methodologies"
	"investigative implications of hardware, OSes and network technologies"
	"system administration, network and operating system hardening techniques"
	"applicable laws, regulations, guidelines, policies and ethics related to cyber security and digital forensics"
	"electronic evidence law, rules of evidence, court procedure and admissibility"
	"processes for collecting, seizing, packaging, transporting, preserving and storing digital/electronic evidence and chain of custody"
	"cyber security and privacy principles"
	"hacking methodologies"
	"cyber threats and vulnerabilities"
	"system and application threats and vulnerabilities"
	"risk management processes (assessment and mitigation)"
	"operational impacts of cyber security lapses"

[79] These are directly quoted from the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse *et al.*, 2017).

	“data backup and recovery”
	“incident response and handling methodologies”
	“application security risks”
	“operating systems including server and client”
	“server diagnostic tools and fault identification techniques”
	“tools, techniques and procedures (including; data carving, search and analysis, security even correlation, anti-forensics, debugging, malware)”
	“deployable forensics”
	“reverse engineering concepts”
	“forensics lab design configuration and support applications”
	“file type abuse by adversaries for anomalous behaviour”
	“malware with virtual machine detection”
Skill	“developing, testing, and implementing network infrastructure contingency and recovery plans”
	“preserving evidence integrity according to standards and procedures”
	“analysing memory dumps to extract information”
	“identifying and extracting data across a diverse range of media and conducting forensic analysis on multiple OSes (e.g., mobile device systems)”
	“collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data”
	“setting up a forensic workstation”
	“using forensic tool suites (e.g., EnCase, Sleuthkit, FTK)”
	“using binary analysis tools”
	“using virtual machines (a range of virtual machines clients)”
	“physically disassembling PCs”
	“deep analysis of captured malicious code (e.g., malware forensics)”
	“one-way hash functions”
	“analysing anomalous code as malicious or benign”
	“analysing volatile data”
	“identifying obfuscation techniques”
	“interpreting results of debugger to ascertain tactics, techniques, and procedures”
Ability	“decrypt digital data collections”
Tasks	“perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis”
	“maintaining deployable cyber defence toolkits to support incident response”

— (taken from Newhouse *et al.*, 2017)

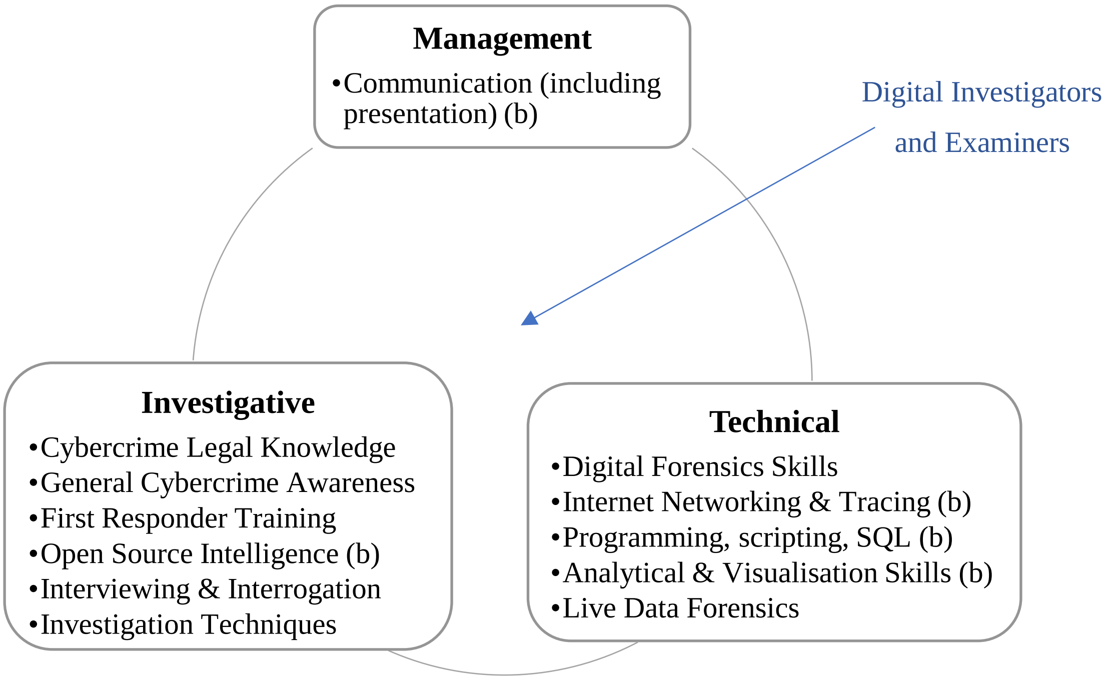
Table F.3.1 – Common Knowledge, Skills and Abilities of a Digital Forensic Practitioner based on the NICE Cybersecurity Workforce Framework

F.4 ECTEG, EC3, CEPOL and Eurojust – Cybercrime Training Governance Model – Cybercrime Training Competency Framework

In contrast to the standards/frameworks above the European Cybercrime Training Competency Framework Cybercrime Training Governance Model highlights three main categories of knowledge and skills required of professionals with roles related to cybercrime in law enforcement, including digital forensics. Of eight roles categorised, four are chosen for analysis due to their relation to digital forensics and cybercrime:

- Digital Forensic Investigators and Examiners;
- Cybercrime Analysts and Intelligence Officers;
- Online Investigators; and
- Heads of Cybercrime Units and Team Leaders.

There is, however, only one role which identifies with digital forensics, while others focus on 'cyber' roles. Each profile is broken down by the level of knowledge and skills required to fulfil the role covering both basic[80] and expert skills. 12 attributes which are common to the four chosen roles are highlighted in Figure F.4.1.


Management
•Communication (including presentation) (b)
Digital Investigators and Examiners
Investigative
•Cybercrime Legal Knowledge
•General Cybercrime Awareness
•First Responder Training
•Open Source Intelligence (b)
•Interviewing & Interrogation
•Investigation Techniques
Technical
•Digital Forensics Skills
•Internet Networking & Tracing (b)
•Programming, scripting, SQL (b)
•Analytical & Visualisation Skills (b)
•Live Data Forensics

— (adapted from Sobusiak-Fischanaller and Vandermeer, no date; Vandermeer, 2018)

Figure F.4.1 – Cybercrime Training Competency Framework: Skills and Knowledge required of law enforcement professionals in roles relating to digital forensics and cybercrime

[80] Basic skills are identified by the key (b).

F.5 Outdated PPF Framework: Digital Forensic Work Profiles

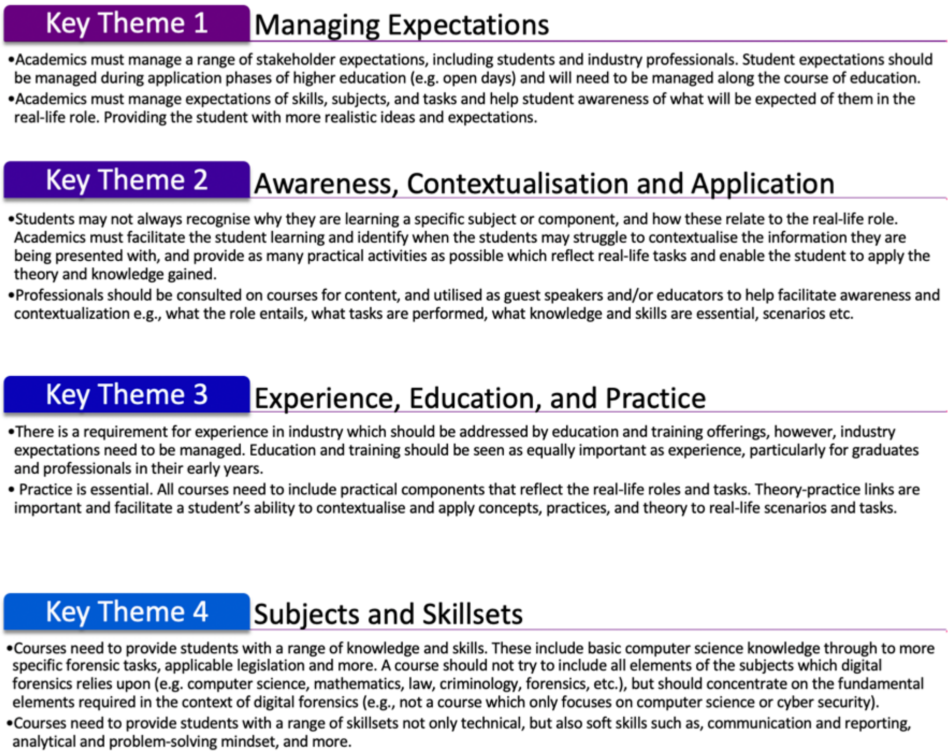
Numerous digital forensic/cyber-related professional roles are outlined in the table below (*Digital Forensics Role Types by the PPF*), according to the old PPF, discussed in chapter 3 (Skills for Justice, 2010b, 2010c, 2011, 2013a, 2013b, 2013c, 2013d, 2013e, 2013f, 2013g).

Role Type	Core Responsibilities
Cyber Investigator Detective Inspector (DI)	- “Conduct Open Source Internet Investigations - Identify and deal with threat and areas of vulnerability - Conduct network investigations”
Cyber Investigator Detective Sergeant (DS)	- “Identify and Secure electronic evidence sources - Seize and record electronic evidence sources - Capture and preserve electronic evidence - Investigate electronic evidence - Evaluate and report electronic evidence - Conduct Open Source Internet investigations - Conduct network investigations - Recover technical equipment”
Cyber Investigator Detective Constable (DC)	- “Identify and Secure electronic evidence sources - Seize and record electronic evidence sources - Capture and preserve electronic evidence - Investigate electronic evidence - Evaluate and report electronic evidence - Conduct Open Source Internet investigations - Conduct network investigations - Identify and deal with threat and areas of vulnerability - Recover technical equipment - Health and Safety in ICT and Contact Centres at Level 1 (L1)”
Cyber Intelligence Development Supervisor DS	- “Conduct Open Source Internet investigations - Conduct network investigations - Identify and deal with threat and areas of vulnerability”
Cyber Intelligence Development Officer DC	- “Identify and Secure electronic evidence sources - Seize and record electronic evidence sources - Capture and preserve electronic evidence - Investigate electronic evidence - Evaluate and report electronic evidence - Conduct Open Source Internet investigations - Conduct network investigations”
Cyber Intelligence Analyst L1	- “Evaluate and report electronic evidence - Conduct Open Source Internet investigations - Conduct network investigations”
Cyber Intelligence Researcher L1	- “Conduct Open Source Internet investigations”
Cyber Infrastructure Officer DC	- “Conduct Open Source Internet investigations - Conduct network investigations”
Hi Tech Crime Unit Manager	- “Currently no NOS attributed to this role”
High Tech Crime Investigator DC	- “Identify and Secure electronic evidence sources - Investigate electronic devices”
Hi Tech Investigation Officer L1	- “Currently no NOS attributed to this role”

APPENDIX G – KEY CONTRIBUTIONS

G.1 Key Themes in Chapter 6 from Analysis of Participant Views

This section is a placeholder for the extended version of Figure 6.6 from chapter 6, and highlights key themes drawn from the analysis of participant responses (e.g. academics, students, graduates, and professionals).



Key Theme 1 Managing Expectations

- Academics must manage a range of stakeholder expectations, including students and industry professionals. Student expectations should be managed during application phases of higher education (e.g. open days) and will need to be managed along the course of education.
- Academics must manage expectations of skills, subjects, and tasks and help student awareness of what will be expected of them in the real-life role. Providing the student with more realistic ideas and expectations.

Key Theme 2 Awareness, Contextualisation and Application

- Students may not always recognise why they are learning a specific subject or component, and how these relate to the real-life role. Academics must facilitate the student learning and identify when the students may struggle to contextualise the information they are being presented with, and provide as many practical activities as possible which reflect real-life tasks and enable the student to apply the theory and knowledge gained.
- Professionals should be consulted on courses for content, and utilised as guest speakers and/or educators to help facilitate awareness and contextualization e.g., what the role entails, what tasks are performed, what knowledge and skills are essential, scenarios etc.

Key Theme 3 Experience, Education, and Practice

- There is a requirement for experience in industry which should be addressed by education and training offerings, however, industry expectations need to be managed. Education and training should be seen as equally important as experience, particularly for graduates and professionals in their early years.
- Practice is essential. All courses need to include practical components that reflect the real-life roles and tasks. Theory-practice links are important and facilitate a student's ability to contextualise and apply concepts, practices, and theory to real-life scenarios and tasks.

Key Theme 4 Subjects and Skillsets

- Courses need to provide students with a range of knowledge and skills. These include basic computer science knowledge through to more specific forensic tasks, applicable legislation and more. A course should not try to include all elements of the subjects which digital forensics relies upon (e.g. computer science, mathematics, law, criminology, forensics, etc.), but should concentrate on the fundamental elements required in the context of digital forensics (e.g., not a course which only focuses on computer science or cyber security).
- Courses need to provide students with a range of skillsets not only technical, but also soft skills such as, communication and reporting, analytical and problem-solving mindset, and more.

G.2 Digital Forensic Roadmaps (Expert Commentary)

This section includes four anonymised transcripts. These are the expert commentary provided by participants in the review of the Digital Forensics Roadmaps discussed within section 9.5.2.

Transcript A

Place of Review:	*Online*	Date of Review:	*22/07/2020*
Interviewee:	*Anonymous*	Interviewer:	*Georgina Humphries*
		Transcribed by:	*Georgina Humphries*

Can you tell me about your experience with digital forensics (either as an academic or, as a professional)?

<Removed not to identify the person> An academic with more than seven years teaching computer science in UK higher education across several institutions. This academic also teaches cyber security modules which include elements of digital forensics.

Researcher: I would like to ask you a few questions about the roadmaps, that hopefully you have had time to look over.

1. **Do you think the roadmaps are applicable to their stakeholder groups?**

Yes. I think that the roadmaps are useful for digital forensics education. They highlight key considerations for program developers as well as the students throughout the studies. As an academic myself I particularly think that the roadmaps for applicants, students, and graduates pin-point items we as academics try to deliver ultimately managing their expectations of a course and by extension, the discipline. We aim to provide them with the fundamental topics and skills that would be useful for all fields and roles within for example, computer science, cyber security, or digital forensics, depending on the course. While we attempt to manage the expectations of applicants, I believe this roadmap highlights crucial questions and stages of research that applicants, students, and graduates should look at conducting before, during and after choosing or completing a course.

2. **Do you think the roadmaps facilitate a student’s journey from applicant to the profession, given your experience?**

I think it is possible that these roadmaps allow the students to think about what they are looking for and learning and facilitates them in identifying specific questions they should ask themselves about their progression and involvement in a course. I think the three key things across the roadmaps are the ability to manage expectations, apply their learning, and be able to contextualise what they have learned with real-life examples and scenarios.

3. **Please describe any enhancements you consider feasible for the roadmaps.**

Educator Roadmap: I believe the educators roadmap could consider the sustainability of courses. The diagram considers those at the stages of development for a digital forensics course from fresh and is a great tool for educators looking to develop a course. However, considering a cycle for sustainability e.g., when do your refresh your courses and how do you go back and repeat some of those steps, that is what I believe could be beneficial.

All Roadmaps Potentially remove the amount of textual content in the graphics themselves and discuss outside the roadmap. Although, I realise that may lose some context for the title points. This is something that should be considered in future versions of the roadmaps.

4. **Do you have any additional feedback or comments?**

I do not. I believe the roadmaps will be very useful to the stakeholder groups and there may even be a potential for a journal article/paper on this topic.

Transcript B

Place of Review:	*Online*	Date of Review:	*20/08/2020*
Interviewee:	*Anonymous*	Interviewer:	*Georgina Humphries*
		Transcribed by:	*Georgina Humphries*

Can you tell me about your experience with digital forensics (either as an academic or, as a professional)?

<Removed not to identify the person> An educator with several years' experience teaching and training topics across digital forensics. Previous experience in industry conducting digital investigations.

Researcher: I would like to ask you a few questions about the roadmaps, that hopefully you have had time to look over.

1. **Do you think the roadmaps are applicable to their stakeholder groups?**

Yes, I think the roadmaps are applicable, and very helpful for the stakeholders.

2. **Do you think the roadmaps facilitate a student's journey from applicant to the profession, given your experience?**

The roadmaps facilitate the perfect student from applicant to become a professional. However, most students do not do all these assessments of the courses before attending a program. Your roadmap will really help students.

3. **Please describe any enhancements you consider feasible for the roadmaps.**

I think when the educator creates a study addressing the placements opportunities should be performed before identifying the placement alternatives (more logical order), and placements programs at companies should be selected based on how well they follow good practice. However, this requires a perfect cooperation with the industry. I also think there were to many panels assessing the course. Would it be better having two? One for the University management/board approval process, and one for the input from industry, students, and graduated together? In addition course surveys is excellent for detecting strengths and weaknesses of a particular course.

I also think the Digital forensic industry is focusing too much on efficiency and their solutions are over dependent on automation, and do not really test their tools. That is why there is a need to select the placements that achieve best practice, or else the students may learn bad practice. I do not think programs need to teach the commercial forensic suites. Post-graduates may attend commercial training courses after finishing the program instead. I think open source tools is better to learn digital forensics. When applying for a position where a specific tool is used as the main tool, they should consider attending training for this tool.

4. **Do you have any additional feedback or comments?**

I think applying current research where it is applicable for the profession is also important. This is especially important because it may help in finding better practice and push the domain forward.

External guest lecturers should be picked based on their relevance, their good practice, and abilities to lecture. Their lectures should follow predefined lecture aims, defined by the course design.

Transcript C

Place of Review:	*Online*	Date of Review:	*21/08/2020*
Interviewee:	*Anonymous*	Interviewer:	*Georgina Humphries*
		Transcribed by:	*Georgina Humphries*

Can you tell me about your experience with digital forensics (either as an academic or, as a professional)?

<*Removed not to identify the person*> An educator with several years' experience in a digital forensic unit. This educator has both hands-on practical and managerial experience in the field of digital forensics.

Researcher: I would like to ask you a few questions about the roadmaps, that hopefully you have had time to look over.

1. **Do you think the roadmaps are applicable to their stakeholder groups?**

I think they are. My main impression is that students who are looking to get into these things are not familiar with what the industry want/are asking for. I think if you look at it the other way, a lot of employers do not know what they want. They do not necessarily have people who are skilled and good in computer forensics, so they do not know what to ask for. In my experience they do not necessarily know the difference between a regular IT specialist and a digital forensics specialist. So, people hiring do not necessarily know what skills they need.

My experience, I did not have the computer forensic experience before. I had management experience. So, I think the biggest problem from my point of view is it is problematic for employers to know what they want, and students do not know what is expected of them. It is not until you are experienced and doing the job that you know what is expected of you, and the skills that are required.

2. **Do you think the roadmaps facilitate a student's journey from applicant to the profession, given your experience?**

I think the roadmap is really good overall. I think it touches on a lot of topics here. I think they are quite good. For example, what you say here about passion and you need to work on things outside the studies and do things outside the curricula is quite good.

The main problem (mentioned above), at the same time a lot of the education in this field is done in a lot of sectors that do not have experience on-the-job. My studies were by people who did not have the practical experience, and they had been taught by people who also did not have the practical real-world experience. The problems given to us were theoretical and they were problems you do not necessarily encounter in the real world, so they were not close to what you do when you start working in the field.

R: How do you think academics could better facilitate these theoretical and practice links?

P: What I would really like here is more collaboration with Police and others alike who have the necessary experience from real-world examples.

R: How may this be achieved between academia and the professionals?

P: Collaboration between universities and the industries needs to be improved. However, I think it is quite hard for the industry to be involved in such collaboration as it is a lot of work and maybe they do not see the potential results.

The private sector is also geared towards income, so I do not see there being much collaboration here as they may not be able to see the benefits. For example, if we look at <university>, I received good feedback from the Bachelor's students when I attended and presented on some of the lessons where they stated they really needed something like this. [I.e., from a practitioner] They had learned a lot at the theoretical level, and they were able to learn about topics such as, Crypto and Bitcoin, but they had not learned how to act on the crime scene with digital evidence. They had the theoretical knowledge. I think the main problem at universities is that they have all the theoretical content, but they provide little of how to use it in practice. That is something <university> benefits from by being a part of both education and the field.

3. **Please describe any enhancements you consider feasible for the roadmaps.**

I think you have addressed quite a lot of the issues. However, it is quite one thing to address it in a roadmap and address it in real-life.

R: Are there any things based on your experience, or in your opinion, that could address this issue [i.e. addressing the points in real-life] quite simply?

P: I believe that some of the computer breaches we have seen over recent years have made people see that we have to address these issues. Take the Maersk hacking example. It is a very interesting story, and it is stories like these that when people and companies get problems and are willing to talk about them, and it is the same with others, I think that it will inflict companies to see they need computer security experts and also computer forensics experts. They can then give us some specific/tailored information as to the people and skills they are looking for. So, when these companies have these problems maybe they will give something back. Students can also learn from these stories too and understand what and why they need to learn certain knowledge and skills.

R: Do you think stories like these enable students to apply their learning better?

P: I think it will help them to see the competences required, and see a practical way of doing things, and that you can apply the theory learned to scenarios and problems that are happening in the real world.

4. **Do you have any additional feedback or comments?**

I think you have addressed things like passion; you cannot underestimate the passion needed to be good in this subject. I do not think you can be good in this discipline if you only go to work or study when told to do so. I have been talking a lot about these in my own work and telling students that they must be passionate and have an interest. They need to work outside their learning, reading forums etc., and have an interest in the subject. I like to see this passion in the roadmap. If anything, maybe the passion should come earlier in the roadmap. You have described this in several places e.g., being active. I actually think it is really good of you to repeat these things.

Yes, for employers… the one thing that could be described here is to make sure you have skilled people to know what they are looking for. Buyers competence – you need to know what you are buying. I know that some CEOs think you can buy computer security in a box. For employers they need to have this buyer and hirer competence. I have interviewed a couple of applicants where myself and others have had the opposite impression. I.e., one thinking the person was talking gibberish and the other thinking the person was highly skilled.

Additional Comments:

Students will often not know much about the requirements or skills the companies are after, and companies, in my experience, will not know to the full extent what they need. People who hire do not always know a lot about computer forensics or computer security. Expectation to computer forensic analysts is (in my experience) built upon what co-workers and admin have seen in films... Most universities do not have good enough live experience. Academia needs to work towards getting people from public and private sectors to have teachers and trainers who are more experienced and who can deliver scenarios that are applicable to the real-world tasks and cases.

I think the educators could benefit from getting people and feedback from industry e.g., real case scenarios. I think the Police could be a lot better at collaborating like this. I think they are also a bit afraid of showing off and telling people what to do. I am afraid that in the case of the police, they are concerned that the bad guys will catch up and be aware of what the Police cannot do. I think the private companies too, do not want to show that they may have had break-ins etc., because of the reduction in market share. For example, there are the Dark numbers – those where they do not tell the Police of break-ins as its timely and they do not get much out of it.

Transcript D

Place of Review:	*Online (Email)*	Date of Review:	*27/08/2020*
Interviewee:	*Anonymous*	Interviewer:	*Georgina Humphries*
		Transcribed by:	*Georgina Humphries*

Can you tell me about your experience with digital forensics (either as an academic or, as a professional)?

<Removed not to identify the person> An educator with several years' experience in a digital forensic unit. This educator has both hands-on practical and managerial experience in the field of digital forensics.

Researcher: I would like to ask you a few questions about the roadmaps, that hopefully you have had time to look over.

1. **Do you think the roadmaps are applicable to their stakeholder groups?**

Yes I do. Some parts of the "Educators" might be a bit resource demanding, but nevertheless I think they should all be there - something to stretch for.

2. **Do you think the roadmaps facilitate a student's journey from applicant to the profession, given your experience?**

I do not think our students follow such a roadmap, not even close. But they are already employed and have a more relaxed approach to doing our courses. However, "ordinary" students might be following a similar roadmap.

3. **Please describe any enhancements you consider feasible for the roadmaps.**

Please see my comments below.

4. **Do you have any additional feedback or comments?**

Please see my comments below.

Additional Comments:

Roadmap	Comments
Educators	1. Start - Should there be a step 0, before Start, to ensure that the idea is a good one? 2. Partnership - What is meant by Industry - does it also include LE? Probably, as it is mention in "Expert Panel" 3. Co-design - ..independent and impartial commentary? 4. University Panel - Probably a good idea as developers often think that course expenses are limited to their own expenses. 5. Expert Panel - What will these experts do? (you do not say) 6. Student Panel - Good 7. Graduate Panel - I see this could be a good idea, but how would you make sure such a panel does not focus too much on quantity and not quality. E.g. in the police they would prefer to hire a person who could reduce their back-log rather than doing a thorough job which takes a lot of time. So, in terms of employability, they would say "Learn how to use Encase and XRY, because that is what is needed". 8. Documenting - Understand the importance of the text there, but how is it related to "Documenting"? 9. Course Info - Spot on 10. Scenario Creation – Agree 11. Placements Alternatives 12. Placements - Should these two be interchanged as the order would be more natural?

	13. Co-delivery - Is "yearly" a too limited phrase. What about "before every delivery" 14. Balancing Expectations - Good 15. Topics - Seem to be quite exhaustive 16. Computing Fundamentals - This is very important. To distinguish between CS and CF is also related to what expectations we give the students. 17. Context & Application - Spot on 18. Practical Learning - Also spot on 19. Crime Scene to Court - Could also be organised throughout the whole course (scenario-based learning) and not just at the end of the course. 20. Employability - Seems to be quite resource demanding. But I guess this could be done at the end of a programme and not after every course.
Applicants	1-8 - Good 9 Course Pre-Materials - This is something [we] could be better at, I think (just a reflection) 10 - Good 11-12 - Swap? 13-16 - Good Ideally I guess that all this information which the students will seek, should be made available prior to the course as it would be quite resource demanding to answer all these questions. So, I see this as a guide also for the course developers.
Students	1-6 - Good 7 - Awareness of tools - Why is this important? Should the education be tool independent? Maybe this is more important the day you start looking for a job, as within the industry there might be a variety of tools in use. More so within LE where special developed tools are in use. I see that this is at an awareness level, but also that they should, to some extent, learn how to use these tools. 8-14 - Good

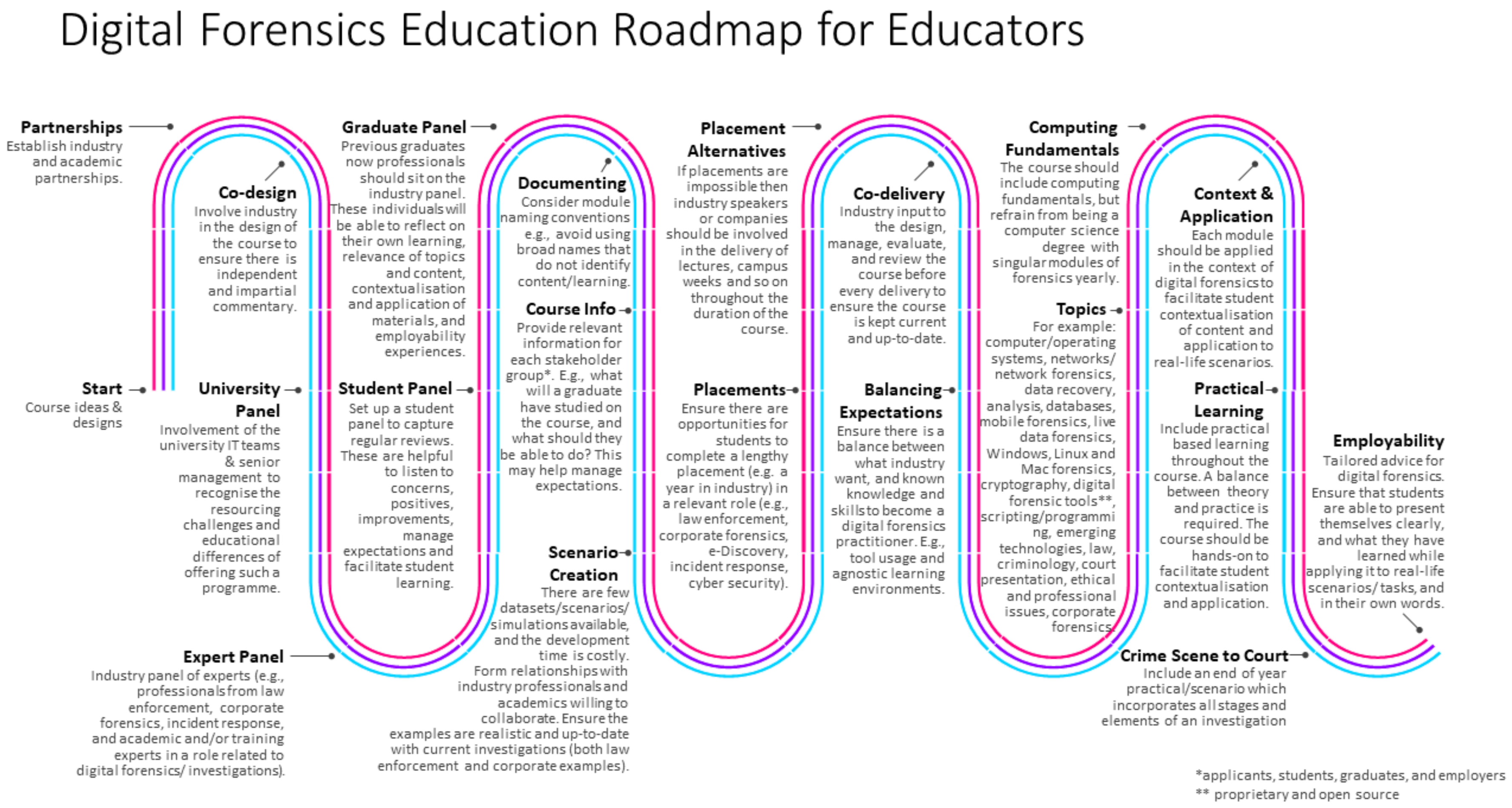
	15 - Employability A bit difficult to relate to [my academic establishment] as they are already employed, but I see the relevance for more "normal" programmes.
Graduates	1-4 - Good 5-7 - Are these meant to be part of the interviewing process, or some sort of a portfolio? 8 - Court Room - This is a good one 9-12 - Same as 5-7
Prof/Emp	1-12 - Interesting 13 - Tool Coverage - I think this text is more nuanced than Student(7). Still I do not see why education should cover well known industry tools (presuming proprietary).

G.3 Final Digital Forensic Roadmaps to Implementing Effective Education

This section holds the final versions of the roadmaps contributed from this thesis. These roadmaps will need to be continuously reviewed to consider the status quo of the digital forensics industry and educations. Themes within these roadmaps are drawn from the analysis of participant responses collated together to provide a roadmap for different stakeholder groups (e.g. academics, students, graduates, and professionals).

G.3.1 Digital Forensic Roadmap for Educators

This roadmap is designed to facilitate the delivery of an academic program in digital forensics delivered by educators.



Digital Forensics Education Roadmap for Educators

Start
Course ideas & designs

Partnerships
Establish industry and academic partnerships.

Co-design
Involve industry in the design of the course to ensure there is independent and impartial commentary.

University Panel
Involvement of the university IT teams & senior management to recognise the resourcing challenges and educational differences of offering such a programme.

Expert Panel
Industry panel of experts (e.g., professionals from law enforcement, corporate forensics, incident response, and academic and/or training experts in a role related to digital forensics/ investigations).

Student Panel
Set up a student panel to capture regular reviews. These are helpful to listen to concerns, positives, improvements, manage expectations and facilitate student learning.

Graduate Panel
Previous graduates now professionals should sit on the industry panel. These individuals will be able to reflect on their own learning, relevance of topics and content, contextualisation and application of materials, and employability experiences.

Documenting
Consider module naming conventions e.g., avoid using broad names that do not identify content/learning.

Course Info
Provide relevant information for each stakeholder group*. E.g., what will a graduate have studied on the course, and what should they be able to do? This may help manage expectations.

Scenario Creation
There are few datasets/scenarios/ simulations available, and the development time is costly. Form relationships with industry professionals and academics willing to collaborate. Ensure the examples are realistic and up-to-date with current investigations (both law enforcement and corporate examples).

Placements
Ensure there are opportunities for students to complete a lengthy placement (e.g. a year in industry) in a relevant role (e.g., law enforcement, corporate forensics, e-Discovery, incident response, cyber security).

Placement Alternatives
If placements are impossible then industry speakers or companies should be involved in the delivery of lectures, campus weeks and so on throughout the duration of the course.

Co-delivery
Industry input to the design, manage, evaluate, and review the course before every delivery to ensure the course is kept current and up-to-date.

Balancing Expectations
Ensure there is a balance between what industry want, and known knowledge and skills to become a digital forensics practitioner. E.g., tool usage and agnostic learning environments.

Topics
For example: computer/operating systems, networks/ network forensics, data recovery, analysis, databases, mobile forensics, live data forensics, Windows, Linux and Mac forensics, cryptography, digital forensic tools**, scripting/programming, emerging technologies, law, criminology, court presentation, ethical and professional issues, corporate forensics

Computing Fundamentals
The course should include computing fundamentals, but refrain from being a computer science degree with singular modules of forensics yearly.

Context & Application
Each module should be applied in the context of digital forensics to facilitate student contextualisation of content and application to real-life scenarios.

Practical Learning
Include practical based learning throughout the course. A balance between theory and practice is required. The course should be hands-on to facilitate student contextualisation and application.

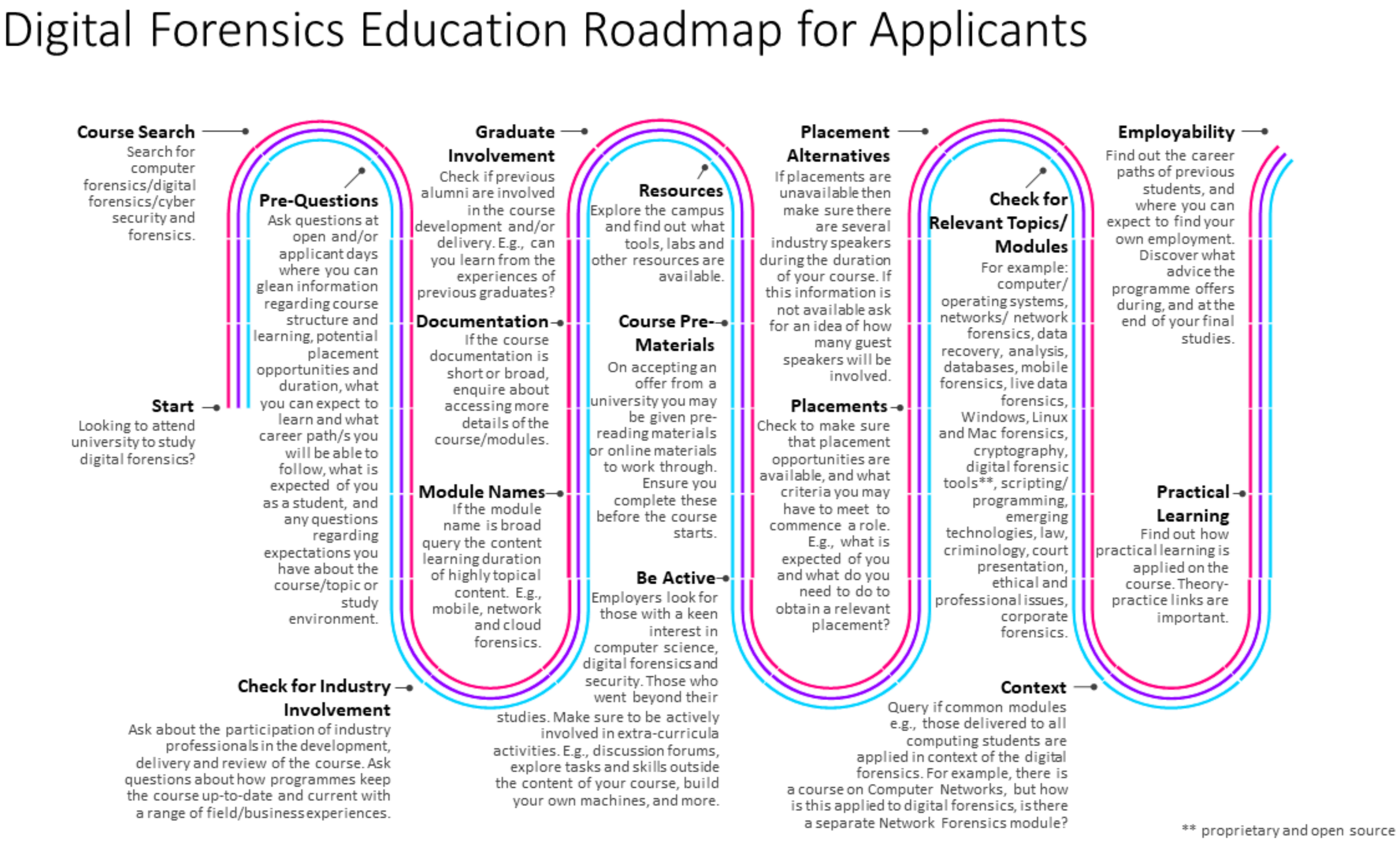
Crime Scene to Court
Include an end of year practical/scenario which incorporates all stages and elements of an investigation

Employability
Tailored advice for digital forensics. Ensure that students are able to present themselves clearly, and what they have learned while applying it to real-life scenarios/ tasks, and in their own words.

*applicants, students, graduates, and employers
** proprietary and open source

G.3.2 Digital Forensic Roadmap for Applicants

This roadmap is designed to facilitate the decision-making process for applicants when looking to study an academic program at HE in digital forensics.



Digital Forensics Education Roadmap for Applicants

Start
Looking to attend university to study digital forensics?

Course Search
Search for computer forensics/digital forensics/cyber security and forensics.

Pre-Questions
Ask questions at open and/or applicant days where you can glean information regarding course structure and learning, potential placement opportunities and duration, what you can expect to learn and what career path/s you will be able to follow, what is expected of you as a student, and any questions regarding expectations you have about the course/topic or study environment.

Check for Industry Involvement
Ask about the participation of industry professionals in the development, delivery and review of the course. Ask questions about how programmes keep the course up-to-date and current with a range of field/business experiences.

Graduate Involvement
Check if previous alumni are involved in the course development and/or delivery. E.g., can you learn from the experiences of previous graduates?

Documentation
If the course documentation is short or broad, enquire about accessing more details of the course/modules.

Module Names
If the module name is broad query the content learning duration of highly topical content. E.g., mobile, network and cloud forensics.

Resources
Explore the campus and find out what tools, labs and other resources are available.

Course Pre-Materials
On accepting an offer from a university you may be given pre-reading materials or online materials to work through. Ensure you complete these before the course starts.

Be Active
Employers look for those with a keen interest in computer science, digital forensics and security. Those who went beyond their studies. Make sure to be actively involved in extra-curricula activities. E.g., discussion forums, explore tasks and skills outside the content of your course, build your own machines, and more.

Placement Alternatives
If placements are unavailable then make sure there are several industry speakers during the duration of your course. If this information is not available ask for an idea of how many guest speakers will be involved.

Placements
Check to make sure that placement opportunities are available, and what criteria you may have to meet to commence a role. E.g., what is expected of you and what do you need to do to obtain a relevant placement?

Check for Relevant Topics/ Modules
For example: computer/ operating systems, networks/ network forensics, data recovery, analysis, databases, mobile forensics, live data forensics, Windows, Linux and Mac forensics, cryptography, digital forensic tools**, scripting/ programming, emerging technologies, law, criminology, court presentation, ethical and professional issues, corporate forensics.

Context
Query if common modules e.g., those delivered to all computing students are applied in context of the digital forensics. For example, there is a course on Computer Networks, but how is this applied to digital forensics, is there a separate Network Forensics module?

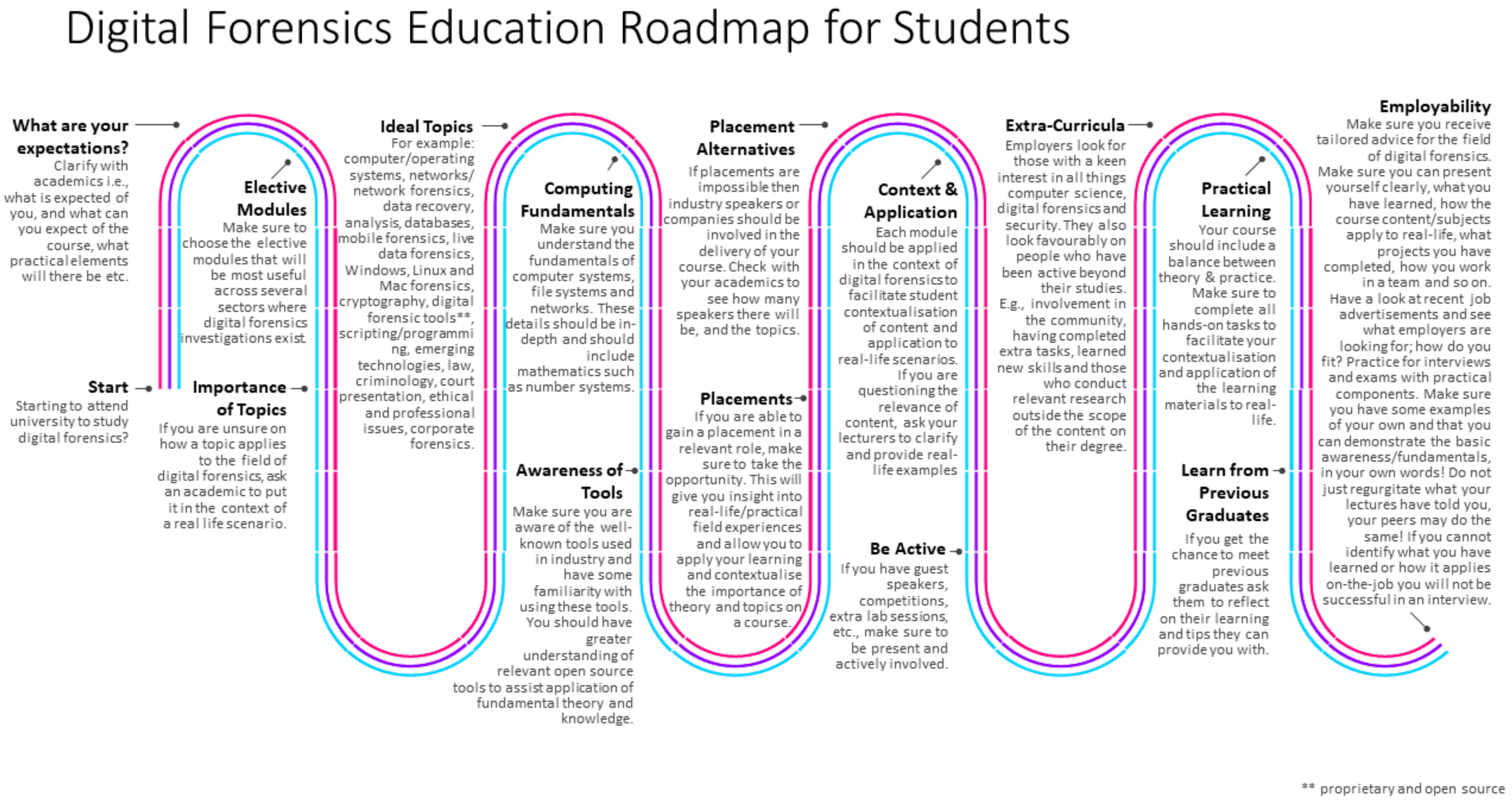
Employability
Find out the career paths of previous students, and where you can expect to find your own employment. Discover what advice the programme offers during, and at the end of your final studies.

Practical Learning
Find out how practical learning is applied on the course. Theory-practice links are important.

** proprietary and open source

G.3.3 Digital Forensic Roadmap for Students

This roadmap is designed to for students already studying on a HE programs in digital forensics and aims to facilitate their decision-making processes and ideally help to manage any expectations.



Digital Forensics Education Roadmap for Students

Start
Starting to attend university to study digital forensics?

What are your expectations?
Clarify with academics i.e., what is expected of you, and what can you expect of the course, what practical elements will there be etc.

Elective Modules
Make sure to choose the elective modules that will be most useful across several sectors where digital forensics investigations exist.

Importance of Topics
If you are unsure on how a topic applies to the field of digital forensics, ask an academic to put it in the context of a real life scenario.

Ideal Topics
For example: computer/operating systems, networks/ network forensics, data recovery, analysis, databases, mobile forensics, live data forensics, Windows, Linux and Mac forensics, cryptography, digital forensic tools**, scripting/programming, emerging technologies, law, criminology, court presentation, ethical and professional issues, corporate forensics.

Computing Fundamentals
Make sure you understand the fundamentals of computer systems, file systems and networks. These details should be in-depth and should include mathematics such as number systems.

Awareness of Tools
Make sure you are aware of the well-known tools used in industry and have some familiarity with using these tools. You should have greater understanding of relevant open source tools to assist application of fundamental theory and knowledge.

Placement Alternatives
If placements are impossible then industry speakers or companies should be involved in the delivery of your course. Check with your academics to see how many speakers there will be, and the topics.

Placements
If you are able to gain a placement in a relevant role, make sure to take the opportunity. This will give you insight into real-life/practical field experiences and allow you to apply your learning and contextualise the importance of theory and topics on a course.

Context & Application
Each module should be applied in the context of digital forensics to facilitate student contextualisation of content and application to real-life scenarios. If you are questioning the relevance of content, ask your lecturers to clarify and provide real-life examples

Be Active
If you have guest speakers, competitions, extra lab sessions, etc., make sure to be present and actively involved.

Extra-Curricula
Employers look for those with a keen interest in all things computer science, digital forensics and security. They also look favourably on people who have been active beyond their studies. E.g., involvement in the community, having completed extra tasks, learned new skills and those who conduct relevant research outside the scope of the content on their degree.

Practical Learning
Your course should include a balance between theory & practice. Make sure to complete all hands-on tasks to facilitate your contextualisation and application of the learning materials to real-life.

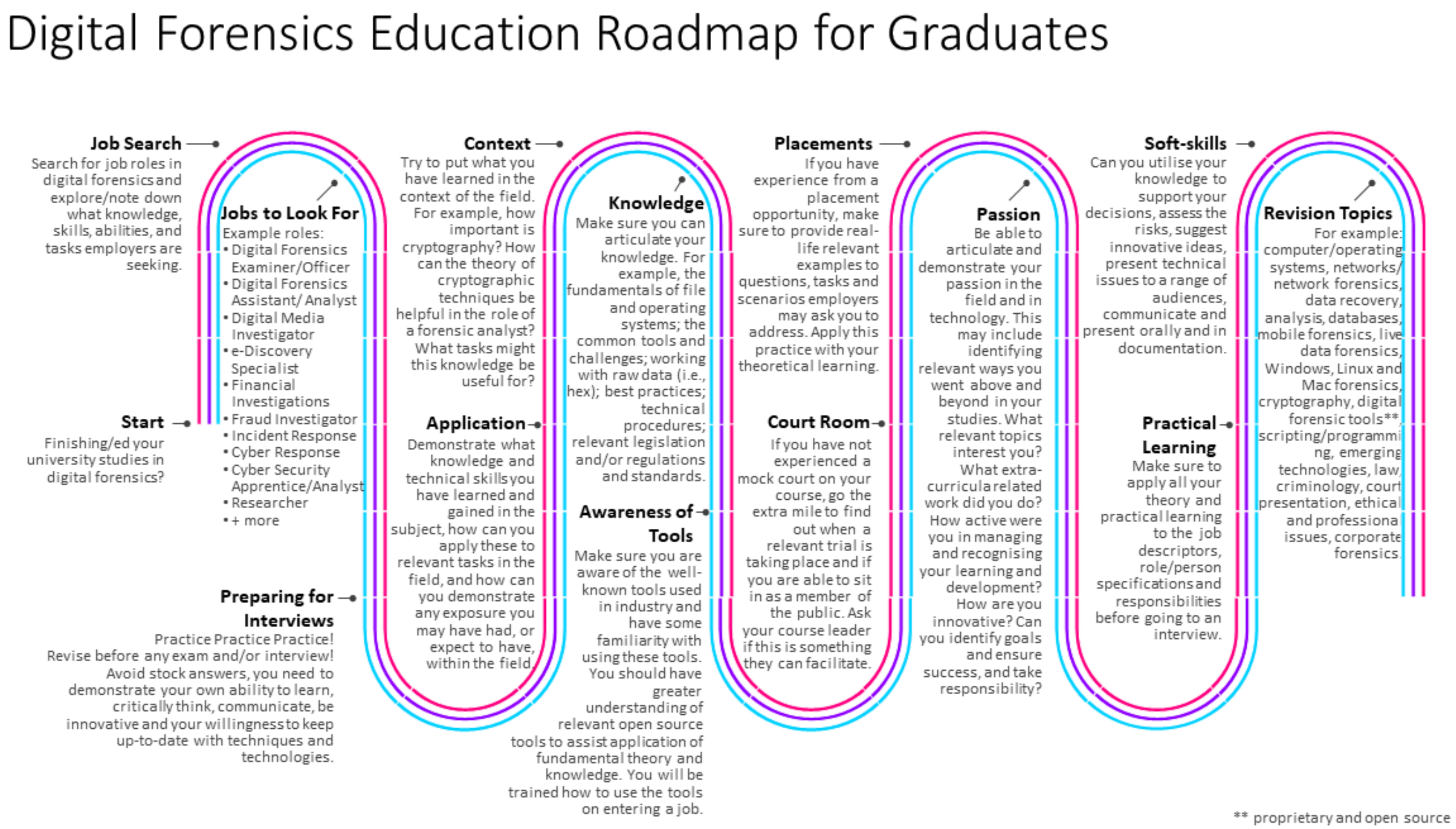
Learn from Previous Graduates
If you get the chance to meet previous graduates ask them to reflect on their learning and tips they can provide you with.

Employability
Make sure you receive tailored advice for the field of digital forensics. Make sure you can present yourself clearly, what you have learned, how the course content/subjects apply to real-life, what projects you have completed, how you work in a team and so on. Have a look at recent job advertisements and see what employers are looking for; how do you fit? Practice for interviews and exams with practical components. Make sure you have some examples of your own and that you can demonstrate the basic awareness/fundamentals, in your own words! Do not just regurgitate what your lectures have told you, your peers may do the same! If you cannot identify what you have learned or how it applies on-the-job you will not be successful in an interview.

** proprietary and open source

G.3.4 Digital Forensic Roadmap for Graduates

This roadmap is designed to facilitate graduates, or students nearing completion of their HE degree in digital forensics and aims to facilitate their decision-making processes and ideally help to manage any expectations to gain employment within industry.



Digital Forensics Education Roadmap for Graduates

Start
Finishing/ed your university studies in digital forensics?

Job Search
Search for job roles in digital forensics and explore/note down what knowledge, skills, abilities, and tasks employers are seeking.

Jobs to Look For
Example roles:
- Digital Forensics Examiner/Officer
- Digital Forensics Assistant/ Analyst
- Digital Media Investigator
- e-Discovery Specialist
- Financial Investigations
- Fraud Investigator
- Incident Response
- Cyber Response
- Cyber Security Apprentice/Analyst
- Researcher
- + more

Preparing for Interviews
Practice Practice Practice! Revise before any exam and/or interview! Avoid stock answers, you need to demonstrate your own ability to learn, critically think, communicate, be innovative and your willingness to keep up-to-date with techniques and technologies.

Application
Demonstrate what knowledge and technical skills you have learned and gained in the subject, how can you apply these to relevant tasks in the field, and how can you demonstrate any exposure you may have had, or expect to have, within the field.

Context
Try to put what you have learned in the context of the field. For example, how important is cryptography? How can the theory of cryptographic techniques be helpful in the role of a forensic analyst? What tasks might this knowledge be useful for?

Knowledge
Make sure you can articulate your knowledge. For example, the fundamentals of file and operating systems; the common tools and challenges; working with raw data (i.e., hex); best practices; technical procedures; relevant legislation and/or regulations and standards.

Awareness of Tools
Make sure you are aware of the well-known tools used in industry and have some familiarity with using these tools. You should have greater understanding of relevant open source tools to assist application of fundamental theory and knowledge. You will be trained how to use the tools on entering a job.

Court Room
If you have not experienced a mock court on your course, go the extra mile to find out when a relevant trial is taking place and if you are able to sit in as a member of the public. Ask your course leader if this is something they can facilitate.

Placements
If you have experience from a placement opportunity, make sure to provide real-life relevant examples to questions, tasks and scenarios employers may ask you to address. Apply this practice with your theoretical learning.

Passion
Be able to articulate and demonstrate your passion in the field and in technology. This may include identifying relevant ways you went above and beyond in your studies. What relevant topics interest you? What extra-curricula related work did you do? How active were you in managing and recognising your learning and development? How are you innovative? Can you identify goals and ensure success, and take responsibility?

Practical Learning
Make sure to apply all your theory and practical learning to the job descriptors, role/person specifications and responsibilities before going to an interview.

Soft-skills
Can you utilise your knowledge to support your decisions, assess the risks, suggest innovative ideas, present technical issues to a range of audiences, communicate and present orally and in documentation.

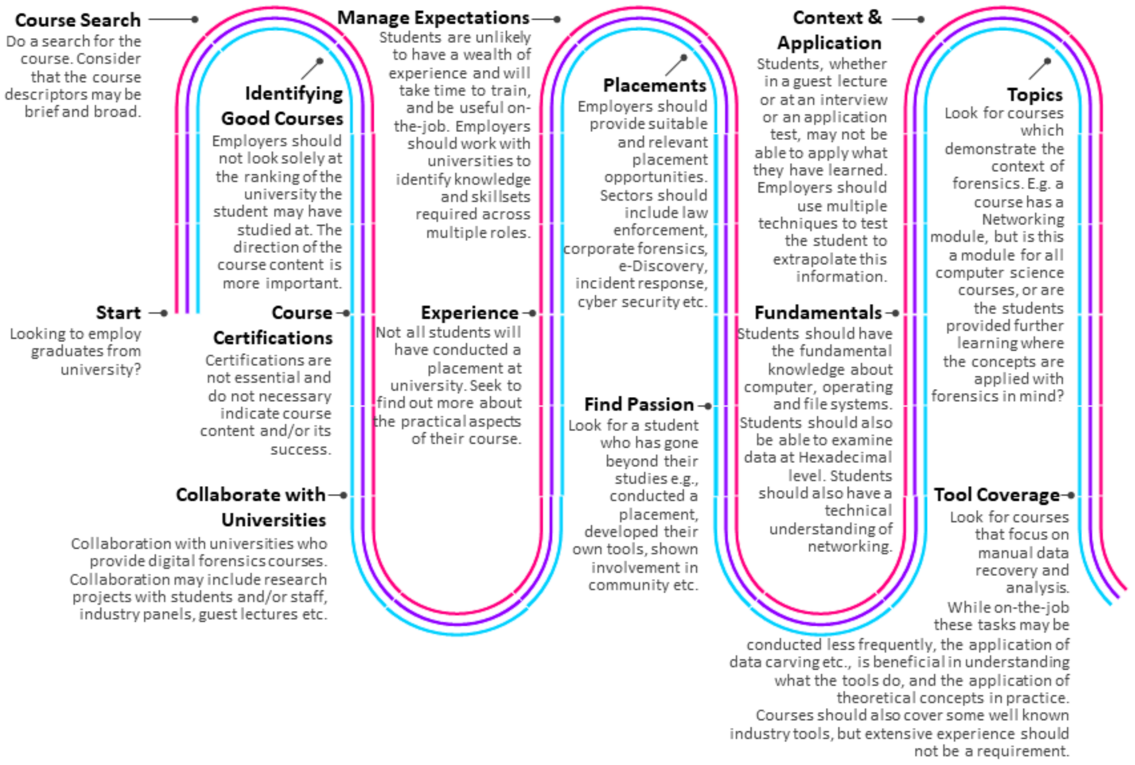
Revision Topics
For example: computer/operating systems, networks/ network forensics, data recovery, analysis, databases, mobile forensics, live data forensics, Windows, Linux and Mac forensics, cryptography, digital forensic tools**, scripting/programming, emerging technologies, law, criminology, court presentation, ethical and professional issues, corporate forensics.

** proprietary and open source

G.3.5 Digital Forensic Roadmap for Professionals/Employers

This roadmap is designed for professionals/employers to facilitate their understanding of key involvement in the academic discipline of digital forensics, collaboration, and the management of expectations of graduates and academia.

Digital Forensics Education Roadmap for Professionals/Employers



Start
Looking to employ graduates from university?

Course Search
Do a search for the course. Consider that the course descriptors may be brief and broad.

Identifying Good Courses
Employers should not look solely at the ranking of the university the student may have studied at. The direction of the course content is more important.

Course Certifications
Certifications are not essential and do not necessary indicate course content and/or its success.

Collaborate with Universities
Collaboration with universities who provide digital forensics courses. Collaboration may include research projects with students and/or staff, industry panels, guest lectures etc.

Experience
Not all students will have conducted a placement at university. Seek to find out more about the practical aspects of their course.

Manage Expectations
Students are unlikely to have a wealth of experience and will take time to train, and be useful on-the-job. Employers should work with universities to identify knowledge and skillsets required across multiple roles.

Placements
Employers should provide suitable and relevant placement opportunities. Sectors should include law enforcement, corporate forensics, e-Discovery, incident response, cyber security etc.

Find Passion
Look for a student who has gone beyond their studies e.g., conducted a placement, developed their own tools, shown involvement in community etc.

Fundamentals
Students should have the fundamental knowledge about computer, operating and file systems. Students should also be able to examine data at Hexadecimal level. Students should also have a technical understanding of networking.

Context & Application
Students, whether in a guest lecture or at an interview or an application test, may not be able to apply what they have learned. Employers should use multiple techniques to test the student to extrapolate this information.

Topics
Look for courses which demonstrate the context of forensics. E.g. a course has a Networking module, but is this a module for all computer science courses, or are the students provided further learning where the concepts are applied with forensics in mind?

Tool Coverage
Look for courses that focus on manual data recovery and analysis. While on-the-job these tasks may be conducted less frequently, the application of data carving etc., is beneficial in understanding what the tools do, and the application of theoretical concepts in practice. Courses should also cover some well known industry tools, but extensive experience should not be a requirement.

APPENDIX H – PUBLICATIONS

PEER-REVIEWED CONFERENCE PAPERS

Humphries, G. (2019) *Public Understanding of Cyber Security and Digital Forensics within the UK.* In: Proceeding of Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019). Nicosia, Cyprus.

Abstract:

Little narrative exists within the literature which focuses on the understanding of cyber security and digital forensics to a much wider audience: the public. This paper's aim is to capture and examine the perceptions of the public by adding insight into what is understood by the terms and disciplines of 'digital forensics' and 'cyber security'. While cyber security and digital forensics can be recognised by their interdisciplinary nature, the two disciplines are distinct in their approach to criminality. At its simplest, cyber security is concerned with the prevention of an incident and implementation of robust systems, while digital forensics focuses on the response to crime and recovering digital evidence. Public perceptions of these areas are important, as security of systems and digital technologies have been heightened in recent years due to high profile cases where notable and large corporations have seen breaches of sensitive information. This study draws on responses from the public using an online survey taken by 102 participants that asked their views on cyber security and digital forensics. This paper demonstrates that there is an awareness among respondents of both disciplines where participants have associated cyber security predominately with the protection of data and systems and digital forensics as the examination and inspection of digital devices. Additionally, responses have also shown there is a need for further awareness in these fields.

Humphries, G. and Williams, J. (2019) *Public Thoughts on Tackling Digital Crime in Society and by Law Enforcement.* In: Proceeding of Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019). Nicosia, Cyprus.

Abstract:

With the ownership of connected digital devices standing at 3 for the average user, the ubiquity of the Internet and the rise in smarter Internet-connected devices, there is an inevitable increase in the rise of digital crime associated with such devices. Well-known is the under-reporting of cybercriminal activities by victims which may give a green light for continued online criminal activities. Yet, there is little focus on the wider public's perception on what needs to be tackled in relation to digital and online crimes; this paper examines and discusses the views of 102 questionnaire responses from public participants. Questions and responses focused on societal challenges surrounding digital technologies and the perception of law enforcement's role in digital and online crimes. Crimes described or listed by participants are coded into themes addressing participant concerns surrounding digital crime. This study also discusses those participants who identified as 'victims of digital crime' (n=25) and offers them to share the actions they took as well as any outcomes. This study found nearly a quarter of respondents have been a victim of dishonest or unlawful behaviour online. This paper speculates how some criminal activities may be under-reported due to lack of awareness alongside the underappreciation for the extent and spread of such crimes. Results show that participants were heavily focused on crimes such as, theft, fraud and those involving children.

Humphries, G. (2017) *Digital Forensics curriculum and training: struggles with a distinct discipline and ontology for learning.* In: Proceedings of EDULEARN17 Conference. Barcelona, Spain: IATED. pp. 8566-8575 ISBN 9788469737774

Abstract:

Digital Forensics has rapidly evolved and developed as an important focus in law enforcement, government, academia and the private sector.

The digital world we live in has had a demonstrable impact on digital forensics; crimes are now accomplished directly involving in-hand devices (e.g. smart devices, wearables, laptop, or tablet) or enhanced by such widely available technological advances. These technologies are at the very fore front of everyday life and becoming more and more integrated into curriculum across Higher Education (HE).

We have subsequently seen the development of a number of education and training courses on offer for not only digital forensics but also cybersecurity. There now exists a plethora of courses in the United Kingdom where, over the years, many Higher Education Institutions (HEIs) have developed 'computer forensics' and 'digital forensics' programmes.

Harnessing new technologies, which such a relatively new and distinctive technological discipline relies upon, includes its own challenges. These include alignment of curricula to current technologies, industry requirements and procedures, resourcing, student satisfaction and increasing demands for innovative learning methods and tools.

A small digital forensics community exists, however, this will need to grow as the field matures. The deliverables of courses, both education and training, are extensive where there is no existing way to measure content and delivery. Furthermore, the new discipline is seeking to combat plagiarism and make student assessment more realistic in the light of limited and costly resources.

This paper examines the current state of digital forensics education, training and learning. It seeks to outline the challenges and predict future implications of technology for an already tech-heavy discipline within digital forensics education in the United Kingdom.

WORKSHOPS

Humphries, G. and Williams, J. (2017) *Effective Training of Investigators for Conducting Open Source Research.* In: 13th Annual Teaching Computer Forensics Workshop, 2nd November, 2017, Sunderland, UK.

Abstract:

Law enforcement officials (LEOs) in the United Kingdom conduct open source research as part of their routine online investigations. Open source research in this instance refers to publicly available information that is available on the Internet. As part of their training, LEOs can attend a Research, Identifying and Tracing the Electronic Suspect course organised by the College of Policing that runs over a five-day period. As part of this training, LEOs are tasked with using the Open Source Internet Research Tool (OSIRT – http://osirtbrowser.com), a free and open source software tool designed to automate and assist with these kinds of investigations. Case studies are used to carry out open source investigations using the tool.

This study, which identifies with both pedagogic and andragogic concepts, looks at the effectiveness of the Research, Identifying and Tracing the Electronic Suspect course, and OSIRT's integration as a training tool for LEOs to conduct open source research. This was achieved by using questionnaires, evaluations and observations while adopting Kirkpatrick's Evaluation Model over a five-day period to twelve LEOs. Much of the course learning adopted techniques such as investigative case studies, problem-based learning, transfer of theoretical knowledge and practical use of tools to assist investigative processes.

Preliminary survey results show that, although participants felt there were challenges with the course, new, applicable skills were learned by all officers. In particular, this study found that OSIRT was well received by LEOs with participant feedback highlighting ease of use, thoroughness and extensive functionality to enhance the investigative process. Furthermore, OSIRT was attributed for helping with the speed of conducting open source research. Results also draw attention to positive impacts participants expect to see as a result of applying the acquired skills back on the job, such as greater confidence, applicable research techniques and a better overall understanding of conducting open source research.

Humphries, G. (2017) *Effectiveness of digital forensics education & training.* In: HEA National Conference for Learning and Teaching in Cyber Security, 5-6 April, 2017, Liverpool.

Abstract:

This poster focusses on the ever-evolving nature of the digital arena surrounding Cyber Security and Digital Forensics. Digital Forensics plays a crucial role in many criminal investigations with Cyber Security no longer being just a buzzword. However, emphasis is placed on the development, and role of, courses within higher education (HE) and businesses across the United Kingdom. With this development, an effective national curriculum and training framework is increasingly necessary. Discourse surrounding integration of Computer Forensics has placed focus towards the teaching of Digital Forensics, but little in the way of collaboration amongst the community within the educational sector.

There is little assurance over the placement of such a multi-/interdisciplinary course, or its position within STEM subjects; where it has yet to define itself. An aspect of this study is to focus on the lack of a national framework and work on producing a framework while also focussing on the effectiveness of teaching and training a Digital Forensics practitioner.

APPENDIX I – RESEARCH ETHICS

This appendix considers the research ethics involved in the process of this study including approval/compliance, informative consent and gaining access to participants.

J.1 Research Ethical Approval

Ethical approval for various research conducted during the time of this thesis study was granted at several phases. Dates for ethical approval are as follows:

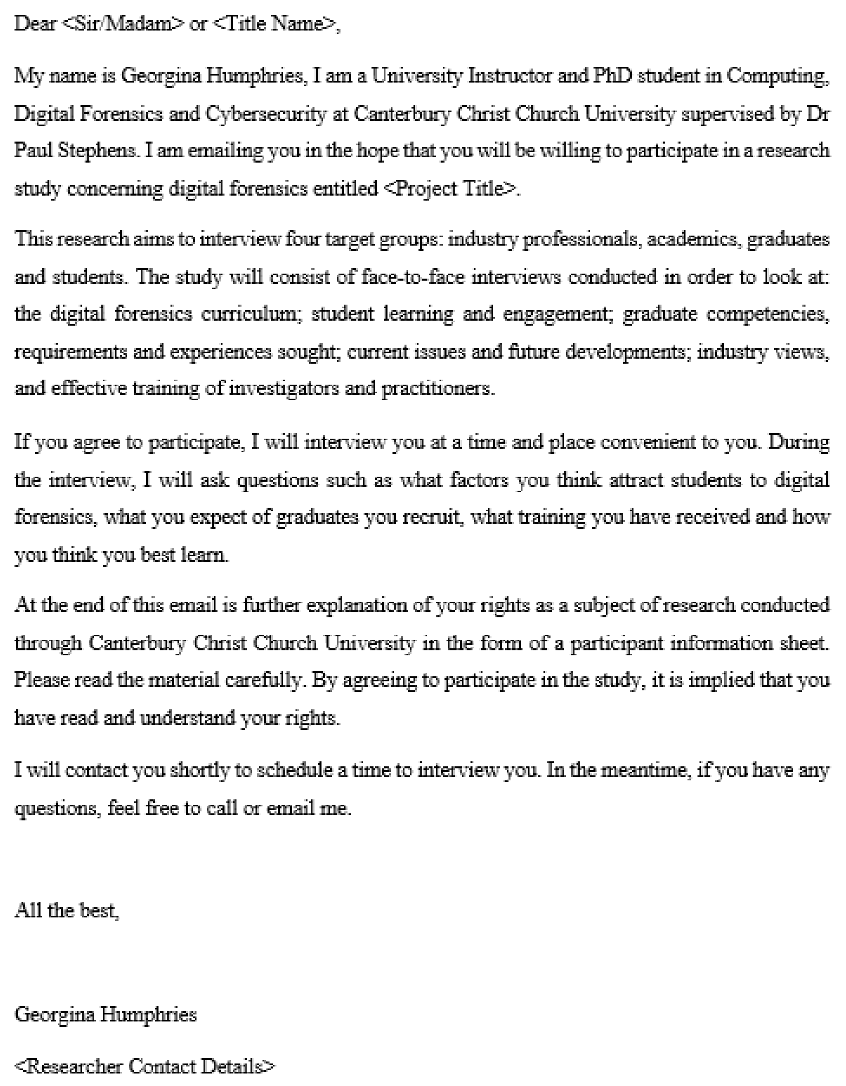
- 29th January 2015
- 3rd August 2016
- 16th August 2017
- 15th September 2017

Compliance with ethical procedures was ensured throughout this study in regulation with Canterbury Christ Church University research terms and procedures. All participants in this study were asked for their consent to elucidate the agreement between the researcher and the participant as well as give permission to involve them in this research. Consent was obtained using either hard copy consent forms and participant information sheets which outlined the participants rights and agreement with the researcher as well as reason for the research. Or, through confirmation after consent/briefing via consent button or checkboxes when conducted online.

J.2 Access Letters

Several methods were utilised throughout this research to gain access to participants. Below outlines information, access letters and/or posts which were used as mechanisms for gaining access to participants.

Example Email Access Letter



Dear <Sir/Madam> or <Title Name>,

My name is Georgina Humphries, I am a University Instructor and PhD student in Computing, Digital Forensics and Cybersecurity at Canterbury Christ Church University supervised by Dr Paul Stephens. I am emailing you in the hope that you will be willing to participate in a research study concerning digital forensics entitled <Project Title>.

This research aims to interview four target groups: industry professionals, academics, graduates and students. The study will consist of face-to-face interviews conducted in order to look at: the digital forensics curriculum; student learning and engagement; graduate competencies, requirements and experiences sought; current issues and future developments; industry views, and effective training of investigators and practitioners.

If you agree to participate, I will interview you at a time and place convenient to you. During the interview, I will ask questions such as what factors you think attract students to digital forensics, what you expect of graduates you recruit, what training you have received and how you think you best learn.

At the end of this email is further explanation of your rights as a subject of research conducted through Canterbury Christ Church University in the form of a participant information sheet. Please read the material carefully. By agreeing to participate in the study, it is implied that you have read and understand your rights.

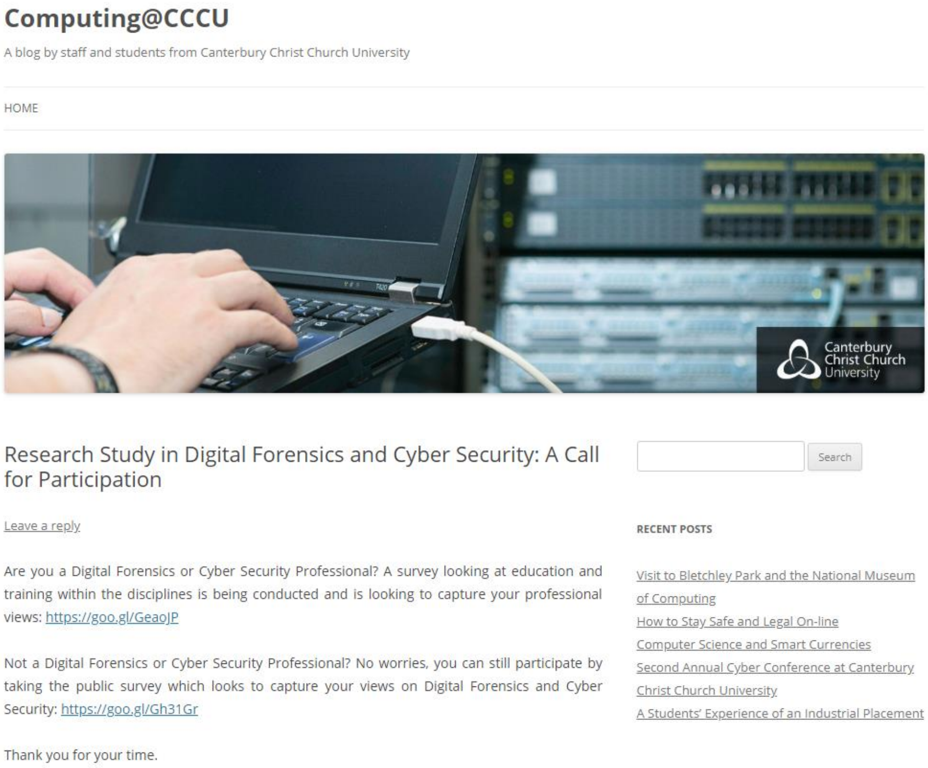
I will contact you shortly to schedule a time to interview you. In the meantime, if you have any questions, feel free to call or email me.

All the best,

Georgina Humphries

<Researcher Contact Details>

Example Social Media Account Posts



Computing@CCCU

A blog by staff and students from Canterbury Christ Church University

HOME

Research Study in Digital Forensics and Cyber Security: A Call for Participation

Leave a reply

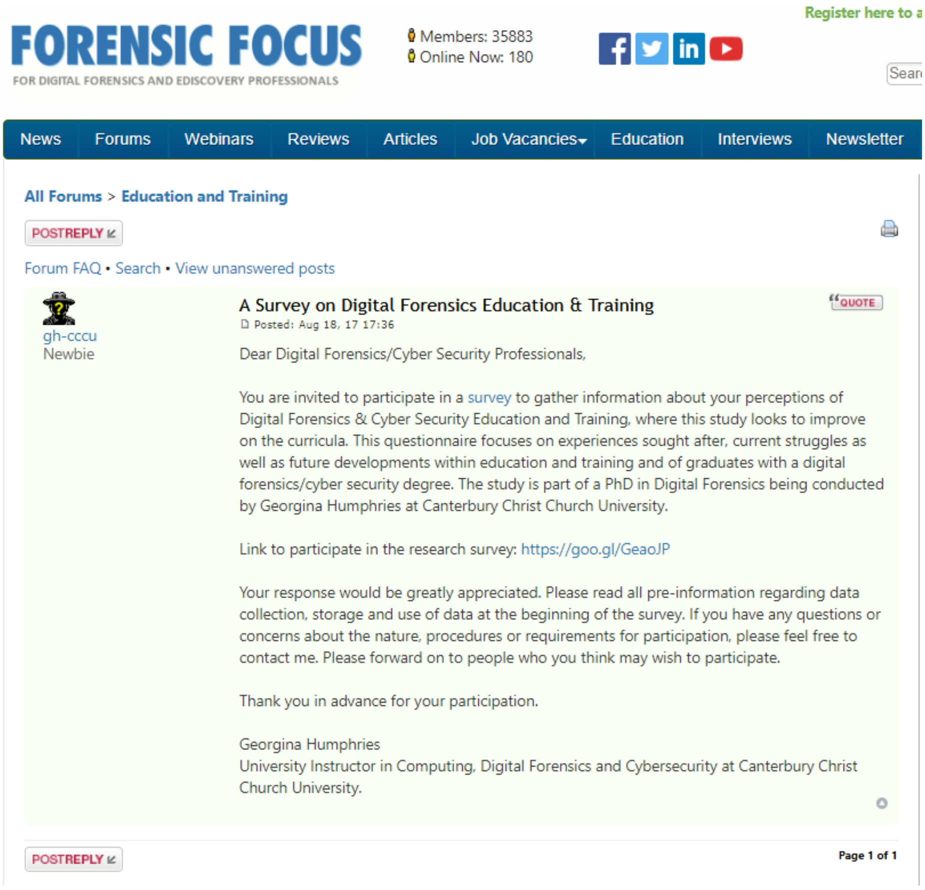
Are you a Digital Forensics or Cyber Security Professional? A survey looking at education and training within the disciplines is being conducted and is looking to capture your professional views: https://goo.gl/GeaoJP

Not a Digital Forensics or Cyber Security Professional? No worries, you can still participate by taking the public survey which looks to capture your views on Digital Forensics and Cyber Security: https://goo.gl/Gh31Gr

Thank you for your time.

Visit to Bletchley Park and the National Museum of Computing
How to Stay Safe and Legal On-line
Computer Science and Smart Currencies
Second Annual Cyber Conference at Canterbury Christ Church University
A Students' Experience of an Industrial Placement

Example Digital Forensic Forum Post



A Survey on Digital Forensics Education & Training

Posted: Aug 18, 17 17:36

Dear Digital Forensics/Cyber Security Professionals,

You are invited to participate in a survey to gather information about your perceptions of Digital Forensics & Cyber Security Education and Training, where this study looks to improve on the curricula. This questionnaire focuses on experiences sought after, current struggles as well as future developments within education and training and of graduates with a digital forensics/cyber security degree. The study is part of a PhD in Digital Forensics being conducted by Georgina Humphries at Canterbury Christ Church University.

Link to participate in the research survey: https://goo.gl/GeaoJP

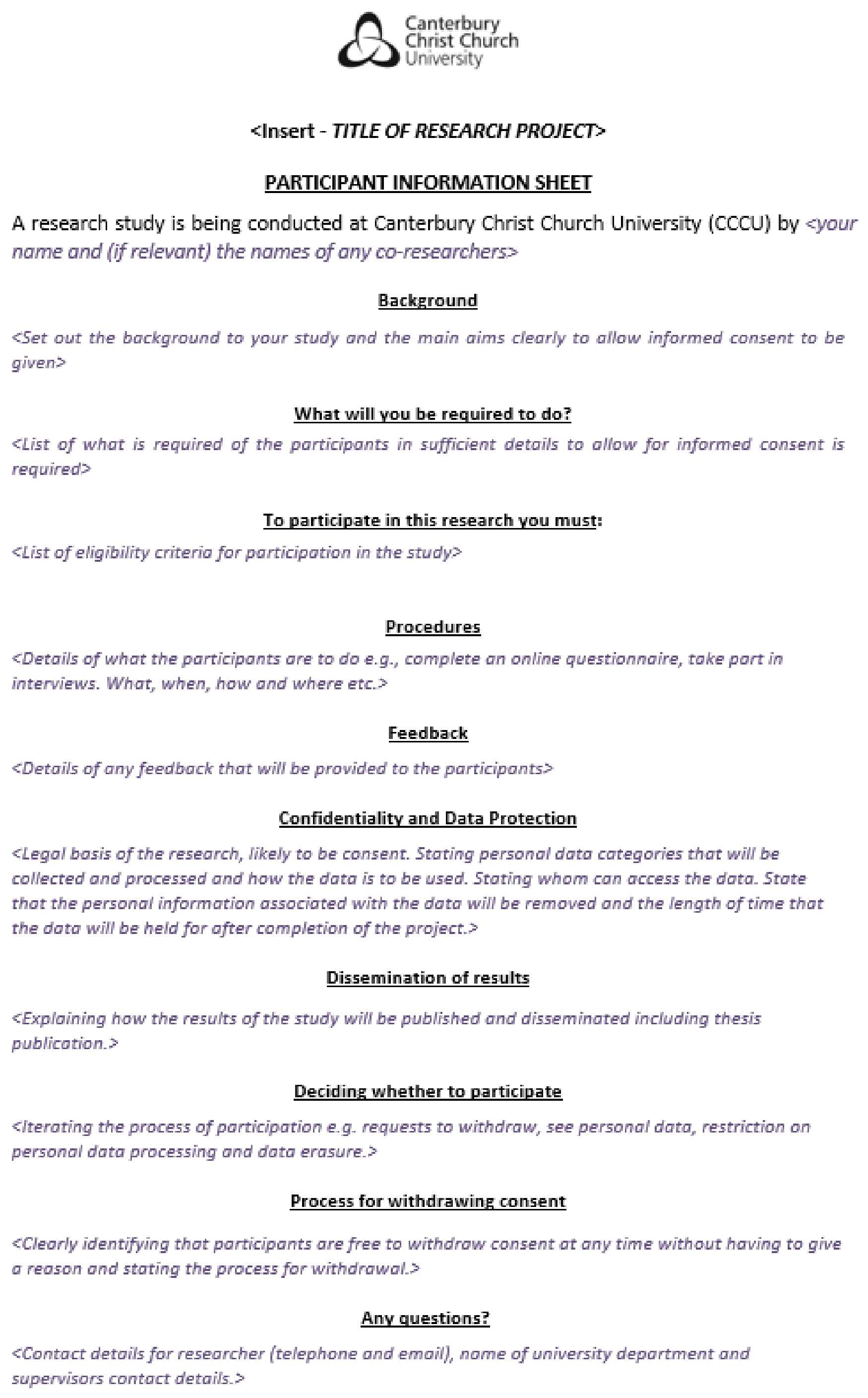
Your response would be greatly appreciated. Please read all pre-information regarding data collection, storage and use of data at the beginning of the survey. If you have any questions or concerns about the nature, procedures or requirements for participation, please feel free to contact me. Please forward on to people who you think may wish to participate.

Thank you in advance for your participation.

Georgina Humphries
University Instructor in Computing, Digital Forensics and Cybersecurity at Canterbury Christ Church University.

J.3 Example Participant Information and Consent Forms

Template for Participant Information Sheet



Canterbury Christ Church University

<Insert - *TITLE OF RESEARCH PROJECT*>

PARTICIPANT INFORMATION SHEET

A research study is being conducted at Canterbury Christ Church University (CCCU) by *<your name and (if relevant) the names of any co-researchers>*

Background

<Set out the background to your study and the main aims clearly to allow informed consent to be given>

What will you be required to do?

<List of what is required of the participants in sufficient details to allow for informed consent is required>

To participate in this research you must:

<List of eligibility criteria for participation in the study>

Procedures

<Details of what the participants are to do e.g., complete an online questionnaire, take part in interviews. What, when, how and where etc.>

Feedback

<Details of any feedback that will be provided to the participants>

Confidentiality and Data Protection

<Legal basis of the research, likely to be consent. Stating personal data categories that will be collected and processed and how the data is to be used. Stating whom can access the data. State that the personal information associated with the data will be removed and the length of time that the data will be held for after completion of the project.>

Dissemination of results

<Explaining how the results of the study will be published and disseminated including thesis publication.>

Deciding whether to participate

<Iterating the process of participation e.g. requests to withdraw, see personal data, restriction on personal data processing and data erasure.>

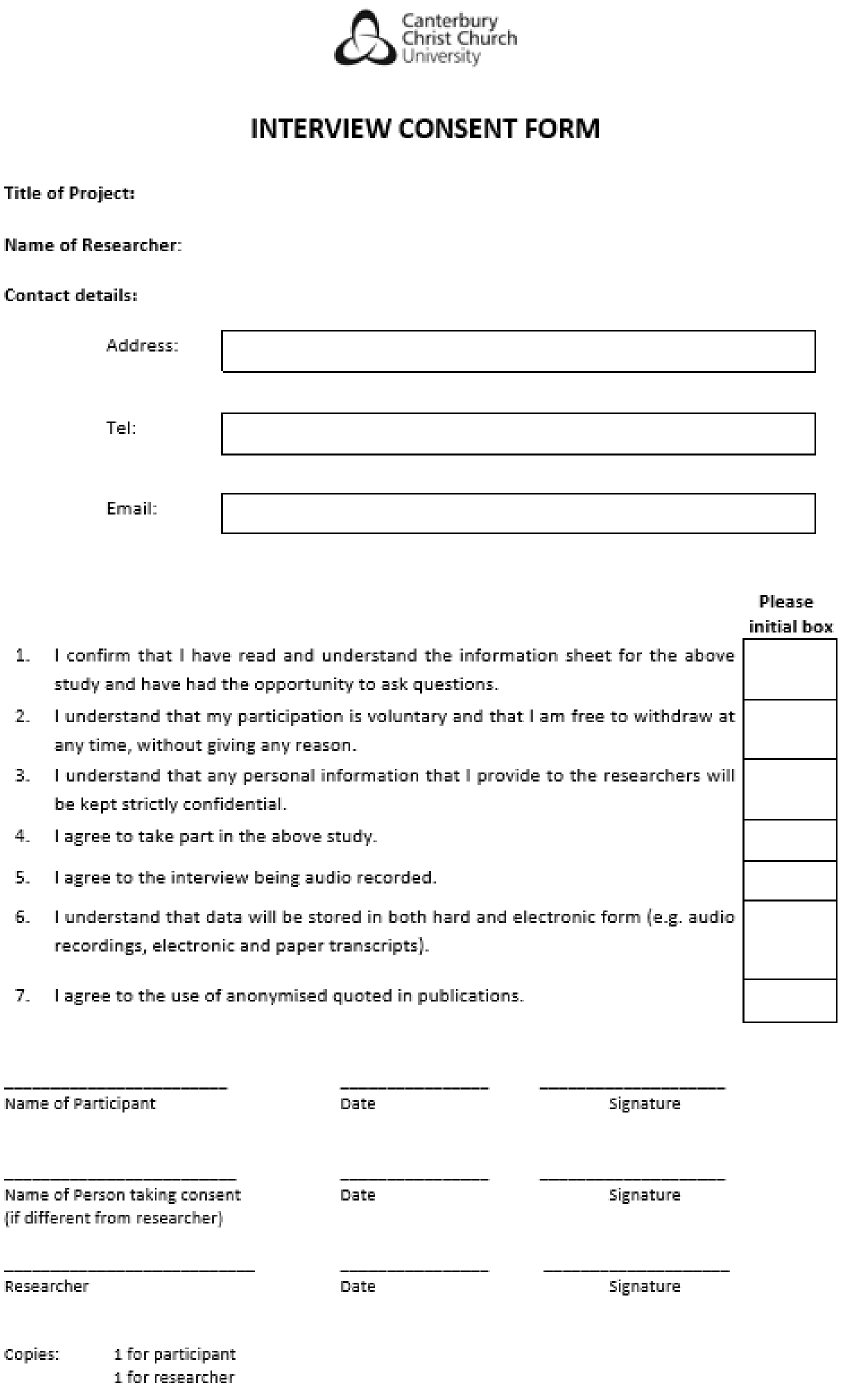
Process for withdrawing consent

<Clearly identifying that participants are free to withdraw consent at any time without having to give a reason and stating the process for withdrawal.>

Any questions?

<Contact details for researcher (telephone and email), name of university department and supervisors contact details.>

Template for Consent Form



Canterbury Christ Church University

INTERVIEW CONSENT FORM

Title of Project:

Name of Researcher:

Contact details:

Address:

Tel:

Email:

Please initial box

1. I confirm that I have read and understand the information sheet for the above study and have had the opportunity to ask questions. □
2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason. □
3. I understand that any personal information that I provide to the researchers will be kept strictly confidential. □
4. I agree to take part in the above study. □
5. I agree to the interview being audio recorded. □
6. I understand that data will be stored in both hard and electronic form (e.g. audio recordings, electronic and paper transcripts). □
7. I agree to the use of anonymised quoted in publications. □

______________________ Name of Participant	_______________ Date	___________________ Signature
_______________________ Name of Person taking consent (if different from researcher)	_______________ Date	___________________ Signature
_________________________ Researcher	_______________ Date	___________________ Signature

Copies: 1 for participant
1 for researcher