University of Bedfordshire

Title: Digital forensics: an integrated approach for the investigation of cyber/computer related crimes

Name: Moniphia Orlease Hewling

DIGITAL FORENSICS: AN INTEGRATED APPROACH FOR THE INVESTIGATION OF CYBER/COMPUTER RELATED CRIMES

MONIPHIA ORLEASE HEWLING

2013

UNIVERSITY OF BEDFORDSHIRE

DIGITAL FORENSICS: AN INTEGRATED APPROACH FOR THE INVESTIGATION OF CYBER/COMPUTER RELATED CRIMES

By

MONIPHIA ORLEASE HEWLING

A thesis submitted to the University of Bedfordshire in partial fulfilment of the requirements for the degree of Doctor of Philosophy

September 13, 2013

DIGITAL FORENSICS: AN INTEGRATED APPROACH FOR INVESTIGATING CYBER/COMPUTER RELATED CRIMES

MONIPHIA ORLEASE HEWLING

Abstract

Digital forensics has become a predominant field in recent times and courts have had to deal with an influx of related cases over the past decade. As computer/cyber related criminal attacks become more predominant in today's technologically driven society the need for and use of, digital evidence in courts has increased. There is the urgent need to hold perpetrators of such crimes accountable and successfully prosecuting them. The process used to acquire this digital evidence (to be used in cases in courts) is digital forensics.

The procedures currently used in the digital forensic process were developed focusing on particular areas of the digital evidence acquisition process. This has resulted in very little regard being made for the core components of the digital forensics field, for example the legal and ethical along with other integral aspects of investigations as a whole. These core facets are important for a number of reasons including the fact that other forensic sciences have included them, and to survive as a true forensics discipline digital forensics must ensure that they are accounted for. This is because, digital forensics like other forensics disciplines must ensure that the evidence (digital evidence) produced from the process is able to withstand the rigors of a courtroom.

Digital forensics is a new and developing field still in its infancy when compared to traditional forensics fields such as botany or anthropology. Over the years development in the field has been tool centered, being driven by commercial developers of the tools used in the digital investigative process. This, along with having no set standards to guide digital forensics practitioners operating in the field has led to issues regarding the reliability, verifiability and consistency of digital evidence when presented in court cases.

Additionally some developers have neglected the fact that the mere mention of the word forensics suggests courts of law, and thus legal practitioners will be intimately involved. Such omissions have resulted in the digital evidence being acquired for use in various investigations facing major challenges when presented in a number of cases. Mitigation of such issues is possible with the development of a standard set of methodologies flexible enough to accommodate the intricacies of all fields to be considered when dealing with digital evidence.

This thesis addresses issues regarding digital forensics frameworks, methods, methodologies and standards for acquiring digital evidence using the grounded theory approach. Data was gathered using literature surveys, questionnaires and interviews electronically. Collecting data using electronic means proved useful when there is need to collect data from different jurisdictions worldwide. Initial surveys indicated that there were no existing standards in place and that the terms models/frameworks and methodologies were used interchangeably to refer to methodologies. A framework and methodology have been developed to address the identified issues and represent the major contribution of this research.

The dissertation outlines solutions to the identified issues and presents the 2IR Framework of standards which governs the 2IR Methodology supported by a mobile application and a curriculum of studies. These designs were developed using an integrated approach incorporating all four core facets of the digital forensics field.

This research lays the foundation for a single integrated approach to digital forensics and can be further developed to ensure the robustness of process and procedures used by digital forensics practitioners worldwide.

Declaration

I declare that this thesis is my own unaided work. It is being submitted for the degree of Doctor of Philosophy at the University of Bedfordshire.

It has not been submitted before for any degree or examination in any other University.

Name of candidate: Signature:

Date:

Dedication

In memory of my mother; M. Jasmine Hall and Grandfather Astley A Hewling

Table of contents

Contents

Abstract ... i

Declaration ... iii

Dedication ... iv

Table of contents ... v

List of Figures ... vii

List of Tables ... viii

Acknowledgements ... ix

DEFINITION OF TERMS ... 1

Abbreviations and Acronyms ... 3

CHAPTER ONE ... 4

INTRODUCTION AND RATIONALE ... 4

1.1 Scope ... 4

1.2 Hypothesis ... 5

1.3 Historical context and current state of digital forensics ... 5

1.4 The Research ... 12

1.5 Assumptions and limitations ... 14

1.6 Previously published material ... 15

1.7 Thesis Structure ... 16

1.8 Summary ... 17

CHAPTER TWO ... 18

DIGITAL FORENSICS AND DIGITAL EVIDENCE ... 18

2.1 Definition and context ... 19

2.2 Legal Context ... 24

2.3 Frameworks/models/methodologies ... 47

2.4 Digital Forensics Tools ... 58

2.5 Digital Forensics Education ... 63

2.6 Summary ... 67

CHAPTER THREE ... 69

RESEARCH METHODOLOGIES ... 69

3.1 Research Approaches ... 69

3.2 Grounded theory 78
3.3 Approach adopted by this study 80
3.4 Initial Survey paper – Phase 3 84
3.4 Summary 97
CHAPTER FOUR 99
The 2IR Framework and Methodology 99
4.1 The 2IR Framework 99
4.2 The 2IR Methodology 132
4.3 2IR Designs Testing 154
CHAPTER FIVE 161
The 2IR Mobile Application 161
5.1 The 2IR Mobile Application Introduction 161
5.2 Analysis Phase 162
5.3 Design Phase 168
5.4 Coding 171
5.5 Testing 182
5.6 Application Review – Discussion of findings 189
CHAPTER SIX 192
CONCLUSION AND FUTURE WORK 192
6.1 Rationale 192
6.2 The Research and its contributions 194
6.3 Transferability and future work. 200
6.4 Direct Contribution to the digital forensics field 200
APPENDICES 202
BIBLIOGRAPHY 233

List of Figures

Figure 1-1 Increase in Cyber crime incidents (2006-2010)..7
Figure 2-1 Area of the digital forensics field comprised in the 2IR designs.................19
Figure 3-1 The process undertaken by this research...80
Figure 3-2 The classification of models from which the 2IR designs are derived..........81
Figure 5-1 Chapter Outline...106
Figure 5-2 Core principles of the 2IR Framework..107
Figure 5-3 Phases of the 2IR Framework...112
Figure 5-4 Core principles of the Initiation Phase..113
Figure 5-5 Core principles of the Investigation Phase..114
Figure 5-6 Core principles of the Reporting Phase...116
Figure 5-7 Facet overview...118
Figure 5-8 Core principles of the facets of the framework..118
Figure 5-9 Principles of the facets and phases of the framework..................................129
Figure 5-10 Stages of the Initiation phase of the 2IR Methodology................................145
Figure 5-11 Stages of the Investigative phase of the 2IR Methodology...........................156
Figure 5-12 Stages of the Reporting phase of the 2IR Methodology................................164
Figure 5-13 Progression in the 2IRCurriculum..169

List of Tables

Table 2-1 The Forensics process……………………………………………………………………...23

Table 3-1 Priority Sequence model…………………………………………………….………………72

Table 3-2 Strengths and weaknesses of collection techniques…………….……………..75

Table 4-1 Background of Participants in the study………………….………………………....85

Table 4-2 How principles within an organization are developed…………………………88

Table 4-3 The distribution of the use of specific digital forensics tools worldwide.90

Table 4-4 The percentage of respondents that use particular tools……………………...91

Acknowledgements

I must say thanks to God for giving me the strength wisdom and insight into undertaking and completing such a challenge.

Having reached the final stages of this research there are a number of persons to whom I am truly grateful for assisting me in getting to this stage. I would like to thank my Director of Studies, Dr. Paul Sant for his constant encouragement and patience, for taking up the enormous challenge of guiding me through this project. Please note I am truly grateful to have had you as my guide.

I must express my gratitude also to my fellow researchers in the Institute of Research in Applicable Computing, special mention must be made of my colleagues Adnan Quereshi, Faisal Quereshi, Kamran Abassi and Ronald Edema. To Kris who always had words of encouragement to keep pressing on. Thank you all.

A big thank you to my church family and personal support group Judith, Kimone, Hilton, Carolyn and Dianne

I could not conclude my acknowledgements without say saying special thanks to the very patient personnel of the Research Graduate School especially Kim who always found a way to help in my times of need.

DEFINITION OF TERMS

This section describes terms associated with the digital forensics field that are used throughout the project that are important to be understood in context.

Ad hoc: This term is often used to refer to make shift solutions with inadequate planning or improvised. It is actually a Latin term meaning 'for this'.

Archive: refers to an accumulation of historical records. May also be used to refer to the space in which these records are held.

ASCII: American standard code for information interchange. This is the standard code used in computer and other digital devices and communication equipment to represent characters.

Baseline Data: this refers to the initial collection of data serving as a basis for comparison with other data sets.

Crime scene: This refers to any location where a crime has taken place.

Cybercrime: This is defined as any offence involving the use of a computer network.

Cyberspace: This refers to the connection and conceptual locations created by computer networks and the World Wide Web.

Computer Crime This is defined to include theft of computer services, unauthorised access to and modification of data and information held on electronic devices as well as software piracy.

Daubert standard: This refers to a test that guides the acceptance of scientific evidence in courts. This test requires meeting five main criteria; Empirical testing: Referring to whether the theory or technique used is refutable, and/or testable. Has the theory used has been subjected to peer review and has it been published? What is the known/potential error rate? Are there the existence and maintenance of standards and controls concerning its operation? What is the degree to which the theory and technique is generally accepted by a relevant scientific community?

Digital Evidence: This term is defined to include any digital data that establish that criminal activity has occurred or provides a link between an accused and victim or accused and crime.

Digital Forensics: this refers to the identification, preservation, acquisition, examination, analysis and presentation of digital evidence.

Evidence: This refers to thing/s that are helpful in forming a conclusion or judgment. Especially used by courts to help judges and juries make decisions in both criminal and civil cases.

Forensic Science (Forensics): This refers to the application of science to investigate and establish the facts related to a case in law (Criminal and Civil).

Framework: a structure for supporting or enclosing something else. A set of assumptions, concepts, values and practices.

Incident: This refers to an event or occurrence usually related to something else.

Investigation: This is the process of investigating which is a detailed enquiry, study or systematic investigation of an incident or thing.

Jurisdiction: This refers to the authority granted to a formally constituted legal body and denotes the geographical area to which this authority applies.

Motive: The need or desire that causes a person to act in a particular way.

Method: A particular form of procedure for accomplishing or approaching something.

Methodology: A set of guidelines used to solve a problem.

Practitioner: This refers to any person actively engaged in an occupation or profession.

Principles: This refers to rules and guidelines to be followed by organisations, groups etc or result in consequences.

Standards: This refers to norm, or requirement of a particular group or organisation.

Triage: This refers to the action of sorting according to quality and usefulness.

Trigger: this is an event that precipitates other events.

Trier of the fact: This refers to the person that determines what the facts are and makes a decision based on those facts in a court of law. Sometimes referred to as the finder of the fact.

Abbreviations and Acronyms

2IR	Initiation, Investigation, Reporting
ACM	Association of Computing Machinery
ACPO	Association of Chief Police Officers
AMEX	American Express
CARICOM	Caribbean Community
CCFP	Certified Cyber Forensics Professional
CEH	Certified Ethical Hacker
CISSP	Certified Information Systems Security professional
CHFI	Certified Hacking Forensics Investigator
CTOSE	Cyber tools Online Search Evidence
DFF	Digital Forensics Framework
DFRWS	Digital Forensics Workshop
DNA	Deoxyribonucleic Acid
EC Council	The International Council of Electronic Commerce Consultants
FORZA	Digital Forensics Investigation Framework incorporating legal issues
FTK	Forensics Toolkit
FRE	Federal Rules of Evidence
HTML	Hyper Text Markup Language
IACIS	International Association for Computers and Information systems
IEEE	Institute of Electrical and Electronic Engineers
IOCE	International Organization on Computer Evidence
IP	Intellectual Property
(ISC)^2	IT Certification and Security Experts
ISO	International Organization for Standardization
IST	Institute for standards in Technology
JDFSL	Journal for Digital Forensics security and Law
NIST	National Institute of Standards and technology
NOS	National Occupational Standards
URL	Universal(Uniform)Resource Locator
USCERT	United States Computer Emergency Readiness Team
VOIP	Voice Over Internet Protocol

CHAPTER ONE

INTRODUCTION AND RATIONALE

The terms digital forensics, forensics computing and computer forensics are often used interchangeably (Schatz 2007). Originally computer forensics and forensic computing referred to the use of computer related evidence in a court of law. Today however the terms digital forensics and digital investigations are frequently used to cover the process by which digital evidence is acquired, examined, analysed and presented in court. This chapter presents an introduction and overview of the work conducted during this thesis and provides the motivation and background material used for this thesis. The chapter begins with a look at the scope of the research followed by the presentation of the research hypothesis. The historical context of digital forensics and its current state are then presented followed by a brief outline of the research, its objectives, relevance and significance and research questions. The assumption and limitations of the research are then highlighted followed by a listing of previously published material and planned publications. The chapter then concludes with an outline of the thesis and a summary of the chapter.

1.1 Scope

This research work aims to ascertain the overall effectiveness of the present digital forensic methods, methodologies and frameworks in dealing with crimes committed involving the use of technologically driven (electronic) devices. Its primary focus is to produce a detailed framework and methodology outlining principles and guidelines to be used in improving the digital forensics process as it exists currently after answering several questions.

Cyber/Computer related crimes have become pervasive in today’s technologically driven society. With the continued increase in the use and availability of digital devices and with previously stored analogue data being made digital, there is the continued need for digital evidence in cases presented in court. The nature of digital evidence makes it different from other types of evidence presented in court, (Schatz 2010) portraying issues of being easily changed, not properly presented along with the general lack of familiarity with evidence of this type. Additionally the process of acquiring this evidence is varied with different models and methodologies of carrying out the process. There also are no existing international standards/principles to guide practitioners in the field worldwide. This process, digital forensics, is still is in its developmental stages as a field and new ways of analyzing and interpreting its resultant digital evidence are constantly being developed and formalised. The work presented in this thesis looks at the field from an integrated perspective, identifying gaps in the field as it relates to standards and procedures in carrying out a digital forensics investigation.

The research will explore the different techniques and methods used by practitioners in the computer/digital forensics field to acquire digital evidence for use in a court of law. It will also discuss the different tools that are available and are used by different digital forensic professionals along with the applicable laws in the field. The research seeks to weigh the pros and cons of the existing models, methodologies and frameworks in place and leads on to the development of a standard set procedures to be used by practitioners in the field will be established. This work presents a case for the absolute need to have a digital forensic methodology that is governed by a framework of principles that may be used as a benchmark internationally. It will also highlight the need for consistency in the field to ensure success in cases involving digital evidence acquisition for legal use. It is founded on the premise that while a framework is an overarching structure providing guidance for a process a methodology is a step by step directive to carry out a process (Hewling 2010).

1.2 Hypothesis

There are a number of digital forensic methodologies existing worldwide. Additionally there are a number of different tools available to assist digital forensic investigators in performing their duties. This has made the acquisition, preservation and presentation of digital evidence an ad hoc process that needs to be standardized. There are no set operating parameters or universal set of standards in use currently for use by digital forensic investigators. This project aims to fill the need for such operating parameters. Hypothesis – That a standardized set of procedures and policies will alleviate some of the issues in cases involving the use of digital evidence.

1.3 Historical context and current state of digital forensics

Cyber/Computer related crime has become a global issue affecting millions of people worldwide. It has become a challenge to authorities as it has facilitated a new wave of criminal activity and criminals which has resulted in a need for practitioners of a new type with additional training to fight this type of crime. The world of virtual crimes presents a new challenge to fields such as criminology, law enforcement, law, Information security among others. The phenomena has changed the entire scope of security and justice systems worldwide who have now had to grapple with the task of restructuring and redefining laws and methods related to the tackling of cyber/computer related criminal activity.

Information security is integral in the prevention of cyber/computer related crimes. With the best of efforts it has become challenging in the dynamic technological age to completely prevent such attacks. Despite the number of security measures that may be in place there are often breaches. Private as well as public entities are challenged with the responsibility of protecting personal data in an era where there is no clear-cut solution to securing computers or related devices. This is mainly due to the fact that cyber/computer attacks come in a variety of different formats which are continually changing in nature. Some of the most highly secured networks of large organizations globally have been known to be breached including Visa Inc and (Octave Klaba) OVH. According to Price Waterhouse the year 2012-2013 showed the highest level ever in security breaches with the cost of several individual breaches costing over one million Great Britain Pounds (GBP) (PWC audit- assurance 2012). The issues faced by companies in securing their systems and, by extension, their data has been a result of the dynamicity of the technology, the increased number and different types of attacks. Cyber crime is not indigenous to any particular region or jurisdiction but affects people worldwide. Additionally its perpetrators may be located anywhere in the world Due to the widespread and increased use of technology along with the increased availability of the Internet worldwide, the environment for committing cyber/computer related crimes has also increased.

The increase in computer related crimes (cyber crime) is “virtually’ unavoidable in today’s technologically driven society. (Kuchta 2000) in looking at the background of Computer Forensics mentions, “Significantly this initiative was born out of the fact that computers were being used to commit crimes more and more”. Connectivity has resulted in a number of security related issues and will continue to do so due to the nature and extensive use of the technology. Cybercrimes have become predominant worldwide as the rapid development of networks and other networked technology especially the Internet grows (Hewling, 2010). Criminals have now become proficient in using technologically based means to commit various types of crimes. Technology based criminal activities include distribution of materials illegally, unauthorized access to computer based material, misuse of computers and the data contained by that computer and using computers as a means of facilitating traditional crimes. Technologically/Digitally driven devices have become pervasive and are deemed indispensible tools by users in a technologically driven society. They facilitate the distribution of information which has become a commodity in its own right. The interconnectivity of these devices enables everyone to have access to more information than they need or want. Additionally they facilitate the storage of personal data and information by individuals and organizations in turn facilitating unauthorized access to data and information that may be used illegally. (Wolf 2003) notes "using the appropriate computing devices, cyber criminals are able to seamlessly conduct malicious or criminal acts through the internet". This point is further supported by (Burden and Palmer 2004) as well as (Giordano and Maciag 2002). Statistics (Figure 1.1) have shown that there has been a significant increase in computer/cyber related crimes in the last decade and thus there is a significant effort on the part of organization and governments to develop and increase measures to tackle the surge.

There is a significant challenge existing with regards to preventing cyber/computer related criminal activity. Despite efforts in the introduction and implementation of security measures including firewalls and intrusion detection systems criminals have become more persistent and always seem to be able to carry out successful attacks against even the most sophisticated systems.

As a response to the need to combat the incidents of cyber/computer related crimes governments and organizations have had to develop a means of conducting investigations into the incidents of cyber related crimes. This investigation though similar to traditional investigations, includes the collection of relevant data, reconstructing the incident scene and creating an intruder profile in an effort to find out who is responsible for the incident and possibly taking legal action.

Computer/Digital forensics is the general term used to denote the acquisition, preservation, analysis and presentation of digital evidence produced in computer/digital crimes. (Kuchta 2000) defines Computer Forensics as "the science that is concerned with the relation and application of computers and legal issues". The goal of computer/digital forensics according to (Carrier and Spattford 2004) is “to identify digital evidence for an investigation”. They continue, “An investigation typically uses both physical and digital evidence with scientific methods to draw conclusions”. (Kerr 2009) suggests that digital forensics combines computer science concepts, including computer architecture, operating systems, file systems, software engineering and computer networking as well as legal procedures that describe criminal and civil litigation, cyber law and rules of evidence. The digital forensics process encompasses identifying activity that requires investigating (including determining pertinent digital sources), collecting information, preserving the information from inadvertent changes, analyzing the information, and reporting the results of the examination, (Casey 2004). Digital/Cyber or Computer forensics as it is sometimes referred, involves the application of science to make the evidence presented in courts clearer.

Forensic science and its related methodologies have been around for centuries however computer/digital forensics is still in its formative stage which presents several challenges in a rapidly developing “digital society”. (Meyers and Rodgers 2004), reiterates, “Computer forensics is in the early stages of development thus problems are emerging that bring into question the validity of computer forensics usage in the United States federal and state courts”. Though efforts have been made to address the situation there are still inconsistencies existing in the field in jurisdictions worldwide. Forensics is defined as “The application of the principles of the physical sciences in the search for truth in civil, criminal and social behavioural matters to the end that injustices shall not be done to any member of society” (White 2010). Generally forensics is the collection and analysis of evidence from an incident scene directly related to an investigation. There has been significant research undertaken resulting in established practices with precise methodologies and techniques for proper handling and analysis of forensic evidence. This extensive research however predates the evolution of digital forensics. (Palmer 2001) notes, “Most forensics disciplines have theories that are published, generally acceptable and testable but digital forensics does not. (Carrier 2006) reiterates, “to date, the digital investigation process has been directed by the technology being investigated and the available tools. While this is acceptable as a temporary measure and suitable if operating independently it is not acceptable if the field is to grow and remain relevant as a forensic science.

In the last two decades there have been a number of developments in the field of digital forensics which is the field that encompasses the acquisition of digital evidence required for cases that are computer/cyber related. Digital/Computer forensic is faced with a number of issues some of which this study will bring to the fore and present amicable solutions. This field encompasses several areas that must be satisfied before the evidence acquired can be accepted in a court of law. These areas include investigative, technical, human relations and legal. The digital/computer forensic investigator has to ensure that at all times the legal aspects of his job are strictly adhered to as this can impact significantly on the outcome of the investigation. This is due mainly to the fact that the general objective of the investigation is to collect, analyze and preserve digital evidence that may eventually be used in courts of law. These factors are also compounded by the rapid changes in technology with which persons engaged in the field have to keep abreast.

The output or result of the digital forensics process is digital evidence. This evidence resides in electronic devices such as computers, digital cameras, tablets, game consoles and mobile phones. These devices are often connected to a network and in-turn the Internet will therefore support digital evidence from internet applications such as emails and social networking activity. The devices also support digital media such as compact disks (CDs), floppy disks, memory sticks, expansion cards, blue ray disks and digital versatile disks (DVDs) which may also contain digital evidence. The use of digital evidence in courts is recent (increasing over the last decade) and thus its acceptability and reliability is constantly under careful scrutiny. The personnel dealing with this evidence at all stages should be trained and knowledgeable in the field. A point is supported by (Casey 2004), "to make informed and proper decisions about the acceptability of digital evidence sources and expert testimony, judges and other judicial panels must be knowledgeable in information and communication technology". Research has indicated however that this is not the case as a number of practitioners in the field are not formally trained to work with digital evidence or to conduct a digital forensics investigation. (Cohen 2008) indicates that all too often the practitioners' knowledge is based on personal experience involving the use of computers and networks such as the Internet as opposed to formal training and education. This situation also presents issues when a practitioner is required to present findings as an expert witness.

Uniformity and consistency in how the evidence is acquired and preserved are primary issues found with digital evidence. It is desired that from this research organizations will realize that it requires much more than a person who is technically inclined to address a digital investigation whether it is routine or criminally motivated. The emergence of cyber crimes has also propelled the need for the development of laws as indicated in the research. These laws have been developed as a part of the solution to combating cyber/computer criminal activity as well as to act as a deterrent. Cyber-laws are described as laws governing actions in cyber space. Cyber laws may fall into any of the following categories:

1. Protection of Privacy
2. Protection of intellectual property
3. Illegal and harmful contents
4. Criminal procedural laws
5. Unauthorized access
6. Computer and financial fraud

Countries worldwide have made great strides in developing laws to address the growing issue of cyber crime. Eg. Singapore Computer Misuse act 19 (1993), Malaysia Computer Crimes Act (1997), Dutch Computer Crime Act (1993), Jamaica Cyber Crime Act (2010). Despite this countries are still faced with the issue of jurisdiction as in a number of cases cybercrime cross jurisdictions with the crime being committed in one country while the perpetrator being located in another. This state of affairs highlights the need for standards and standardization in the way the digital evidence used in the administration of these cases is acquired. Such is the foundation of this research project. The desire to ascertain a standard procedure which if followed meticulously and incorporates the use of the appropriate tools will result in the digital evidence acquired being more robust court of law.

Digital forensics "aims to solve, document and enable the prosecution of computer related crimes" (Huebner et al 2007), and due to its very nature includes practitioners from different fields. This includes, law enforcement personnel, legal personnel, technical personnel from a computer science or information technology background as well as the management of organizations. The acquisition of digital evidence, the end product of the digital forensics process has to comply with not only technical standards but also investigative and legal standards. This culmination of fields presents digital forensics with some issues including that of standardization in the way the process is executed as well as the conditions under which it is performed.

Digital forensics is inherently different from the other forensics disciplines in that it requires different tools and also involves a range of digital devices. It, like the other forensics fields require specialized training and education. Digital Forensics like other forensic fields also requires consistency and standards.

(Mitchison 2005) hypothises;

> *"if only all investigators used the same approach, from sys admins and IT security specialist right through to police or we could be sure that the same approach would be followed by investigators in other jurisdictions; And if only the companies running e-services had systems running which could prove what was going on".*

A number of organizations have developed guidelines, methodologies and frameworks for the field of digital forensics, however as alluded to before there is no one set that has been universally accepted. These include National Institute of Standards and Technology (NIST) that produced a 'Guide to Integrating Forensics Techniques into Incident Response and the Association of Chief Police Officers (ACPO) that produced a set of guidelines to be observed by practitioners when carrying out the digital forensics process.

The European Commission's IST programme in 2003 supported the CTOSE (Cyber Tools On Line Search Evidence)project sponsored by three Universities, two research and development organizations and two commercial companies, this to develop a methodology, architecture, process model, and a common set of tools and procedures for electronic investigations. It was hoped that this set of documents could become a benchmark however (Huebner et al 2007) notes that the project closed in the September 2003 without delivering any obviously significant results or input to the field with a promise of further development. Such instances support the view that digital forensics is still in its infancy without any clear direction with regard to being developed as a true forensics field. This research presents a comprehensive set of designs that encapsulates all the facets of the digital forensics field into one integrated approach which could effectively replace all existing digital forensics methodologies/frameworks/models. The research outputs eliminate the existing issues with the digital forensics process producing designs that integrate legal, technical, ethical and education considerations into a simplified document ensuring adherence to legal and ethical standards when properly used.

The lack of standardization in the field is one of the many issues with which it has to grapple. In 2003 Marc Rogers noted in a security magazine 'Security Wire Digest' that,

> *"In order for Computer Forensics to be a legitimate scientific discipline, it must meet the same standards as other forensics sciences. These include formal testable theories, peer reviewed methodologies and tools and replicable empirical research. Sadly, these standards are not being met."*

In spite of the fact that the field has come a long way since then there is much more to be done. (Huebner et al 2007) reveals that, there have been many attempts made to formulate a set of standards, however none of these have been commonly accepted neither are they updated as often as the field would require.

1.4 The Research

This research has as its main focus the aim of creating a digital forensics framework (integrated) from which a detailed methodology (prescriptive) will be derived to be used by practitioners (Lawyers, Computer Security personnel, Law enforcement officers) in the field when investigating incidents involving digital technology, computers and related technology and/or committed in cyberspace. The key output will be the framework with a derived methodology complete with a set of standards comparable to others in the general forensics field which will serve as the benchmark for digital forensic practitioners whatever their specialization, a set of standards that will ensure that digital evidence acquired will be resilient in a court of law. This solution will be supported by empirical evidence produced from data collection and analysis to ensure its relevance to practitioners in the field. The research methodology to be used throughout the thesis includes a combination of methods, both qualitative (existing literature) and quantitative (interviews and questionnaires), to gather data from digital forensics practitioners. This research employs a combination of research methodologies and paradigms throughout its duration. This was done to ensure that there was a rich set of data as a combination of methods are deemed to produce much more than one method can on its own.

The research will take a detailed look at the different methods, procedures and tools employed by digital forensics investigators from different academic backgrounds in acquiring digital evidence. The need for standardization will be explored and the solutions include a devised tool accompanying the methodology supported by empirical evidence to show benefits to the practitioner. These are solutions designed with the objective of being a benchmark for digital forensic practitioners from different specialist backgrounds and to ensure that digital evidence acquired will be resilient in a court of law.

The research will have as a focus the aim of ascertaining the overall effectiveness of the digital evidence presented in courts to deal with crimes committed using a digital devices and/or computer related technology. It will propose the development of a detailed methodology eliminating gaps present in existing methodologies, which will be governed by a set of standards in a framework for use by practitioners in the field.

To ensure validity of scientific evidence in courts there is a particular set of standards that need to be met. These are based on the Daubert standards arising from the Daubert v Merrell Dow case, 509 U.S 579 (1993). It is clear that for digital forensics to be recognised as a true division of the forensic science arena the evidence gathered through the process must be able to satisfy particular conditions such as those set out in the Daubert testing criteria.

Objectives of the project

1. To develop common code of practice for the digital forensics community that will bridge the divide presented in major court cases where the evidence for the crime/s resides in the digital realm.
2. To devise a comprehensive methodology that will allow computer forensic practitioners to capture and preserve digital evidence acquired adequately, keeping in mind the volatility of the data.
3. To develop a framework of standards/principles addressing the legal, technical, investigative and educational issues that will help to ensure more widespread admissibility of digital evidence in courts and increase integrity.

Research Contribution

This thesis will add to the body of knowledge regarding digital forensics building upon existing research as it relates to models and frameworks in the field producing a set of policies guiding the acquisition of digital evidence. Additionally it contains an extensive review of the existing digital forensics methodologies. This thesis by producing a set of standards/principles to guide a developed methodology provides a foundation for the development of an international set of standards for the digital forensics process that may be used ensure formalization in the acquisition of digital evidence.

Relevance and significance of the study

1. It addresses the problematic area of standardization in the acquisition of digital evidence produced by the digital forensics process.

2. It addresses areas that have not been collectively addressed before by any previous methodology. (Legal, Ethical, Technical, Educational.)

3. It address all areas of digital forensics (digital devices) which has not been done before as a whole. Previous methodologies were developed focusing on a particular area of the digital domain such as mobile, network, computers or Internet.

4. It will be a prescriptive methodology supported by a framework of standards/principles recommending particular tools for use at different stages throughout.

Research Questions

1. To what extent would a common code of practice for digital forensics practitioners help to bridge the divide in major court cases where the evidence resides in the digital realm?

2. How could the development of a standardized methodology in the field allow computer forensics practitioners to capture and preserve digital evidence acquired adequately, keeping in mind the volatility of the data?

3. Would a framework of standards governing the acquisition of digital evidence acquired through the digital forensics process help to make this evidence more robust in court.

4. To what extent would a methodology governed by a set of standards help to alleviate issues encountered by digital evidence (results of the digital forensic process) when presented in court of law.

1.5 Assumptions and limitations

The research is founded on no previous assumptions with respect to the content of the findings. Other assumptions included the fact that it was assumed that the participants in all sections of data gathering would have been interested in seeing the field being formalised and interested in outputs from the project and thus would provide genuine and honest responses. Limitations in the conducting of the research that may have impacted the validity of the study included:

Participants in the research were volunteers and thus their responses may not be representative all practitioners in the field. Additionally because they were volunteers they could drop out at anytime even after agreeing to participate in the study (Carlton 2006).

Participants were from different cultural background and thus the willingness to be interviewed after testing the deliverables varied. Some participants did not understand why they could not only send an email with their findings as opposed to an interview (which they thought unnecessary and inappropriate).

Not all the participants in the testing of the deliverables were part of the cohort who did the initial survey questionnaire.

The grounded theory method was used and thus the existing literature surrounding digital forensics methods, methodologies frameworks and standards were explored before forming a hypothesis.

1.6 Previously published material

Conference presentations and peer reviewed publications:

- Hewling M.O. Sant P. (2012) Digital Forensics: An Integrated approach, Proceedings from 6th Cybercrime Forensics Education and Training, Canterbury Christchurch University, Canterbury, UK
- Hewling M.O. Sant P. (2012) An integrated approach to investigating computer related crimes, UOB'12 Going for Gold, Academic Conference, University of Bedfordshire, Luton, UK, Poster Presentation, UOB'12
- Hewling M. O., Sant P., (2011) Digital Forensics: the need for integration, Workshop on Digital Forensics and Incident Analysis proceedings, WDFIA 2011.
- Hewling M. O., Sant P., (2011) Digital Forensics: The legal Framework. University of Bedfordshire Conference 2011 proceedings, UOB'11
- Hewling M. O., Sant P., (2011) Digital Forensics: A Combined Framework. University of Bedfordshire Conference 2011 Poster Presentation, UOB'11

Planned Publications 2013/2014

Hewling M. O., Sant P., (2013/14) Investigating Cyber crimes; A Caribbean perspective.

Hewling M. O., Sant P., (2013/14) Towards developing Digital Forensics as a true forensics science

1.7 Thesis Structure

The thesis will take the following format. Chapter two will present a review of the existing literature related to the facets of the digital forensics field that are being investigated by the project. The chapter begins by outlining the concept of forensic science from which digital forensics is derived. Here the definition and key terms as they relate to the forensic sciences are explored. The area of crime scenes, their purpose, function and treatment in the event of an investigation are then probed. The chapter continues with exploration of the legal facet of forensic science and how digital forensic is impacted by then discussing specific laws and presentation of previous cases involving digital evidence. The chapter concludes with a look at the previous models/frameworks/methodologies developed in the field, identification of any short comings as well as any highlights.

The third and fourth chapter looks at the research methodology and findings of the project. Chapter three discusses different research approaches analysing their strengths and weaknesses. It then presents the research methodologies employed by the project and the rationale for the choice. Chapter four discusses the findings of the project resulting from methodologies used. It presents a discussion of the initial survey undertaken, the questionnaires developed and the interviews.

The fifth chapter presents the outputs from the research. The main outputs being the 2IR Framework and Methodology which are supported by a developed curriculum for training practitioners in the field as well as an application (2IR APP) for use with the methodology. 2IR being the acronym for the phases of the framework and methodology, Initiation, Investigation and Reporting. The Curriculum is designed for three levels of qualification, Certificate, Undergraduate and postgraduate. It also includes recommendations for research studies.

Chapter six presents an overview of the entire project and includes the future work and contribution of the study. This is then followed by the Appendix and list of references. The appendices include the coding for the application, samples of output documents as well as sample plans to be used by the practitioner.

1.8 Summary

The dynamic nature of technology combined with the increase in its use by members of society has resulted in the increased security breaches and the need for digital forensic services. Digital forensics has become increasingly popular over the last decade due to the increased presence of digital evidence in courts across jurisdictions in both criminal and civil cases (Cohen 2008), (Kessler 2010). To ensure acceptance in court digital forensic must meet the standards required of evidence in courts such as Daubert, (1993). For there to be satisfactory compliance with standards such as Daubert's there has to be set format for the production of digital evidence. The development of the framework and accompanying methodology encompassing the core facets of the field that may be used as a benchmark for practitioners in the digital forensics field and will address the existing issues regarding the process of digital evidence acquisition and its use in courts.

This research and its output will contribute to an improvement in the digital forensics process with the standardization of the process of acquiring digital evidence for use in courts. The research also aims to contribute to the development of the field as a true forensics discipline with the integrated development of a framework of standards governing a methodology accompanied by a mobile application. These integrated designs are founded on the core facets of digital forensics ensuring adherence to legal and ethical principles thus providing more reliable, accurate and verifiable digital evidence.

CHAPTER TWO

DIGITAL FORENSICS AND DIGITAL EVIDENCE

This chapter presents a review of literature related to digital forensics. It will begin by exploring the context of forensic science looking at its history and definitions. The general concept of forensic science and crime scenes will be explored as well as their applicability in digital forensics. The chapter then continues with an in-depth look at the legal context covering the evidence and admissibility, digital evidence, legal issues and laws. Digital forensic tools and education which are also critical facets to this research are then explored. Digital Forensics tools are integral to the digital forensics process and their function and the role they play must be explored with regards developing a guide to the process. Education and training are integral factors to the performance of a digital forensics professional and thus must also be explored throughout the development of a digital forensics framework of standards. The chapter ends with a look at previous work undertaken in the field with a focus on methodologies, frameworks and models including works such as (Carlton 2007), (Casey 2011) and (Kessler 2010) whose work underpins much of the research covered.

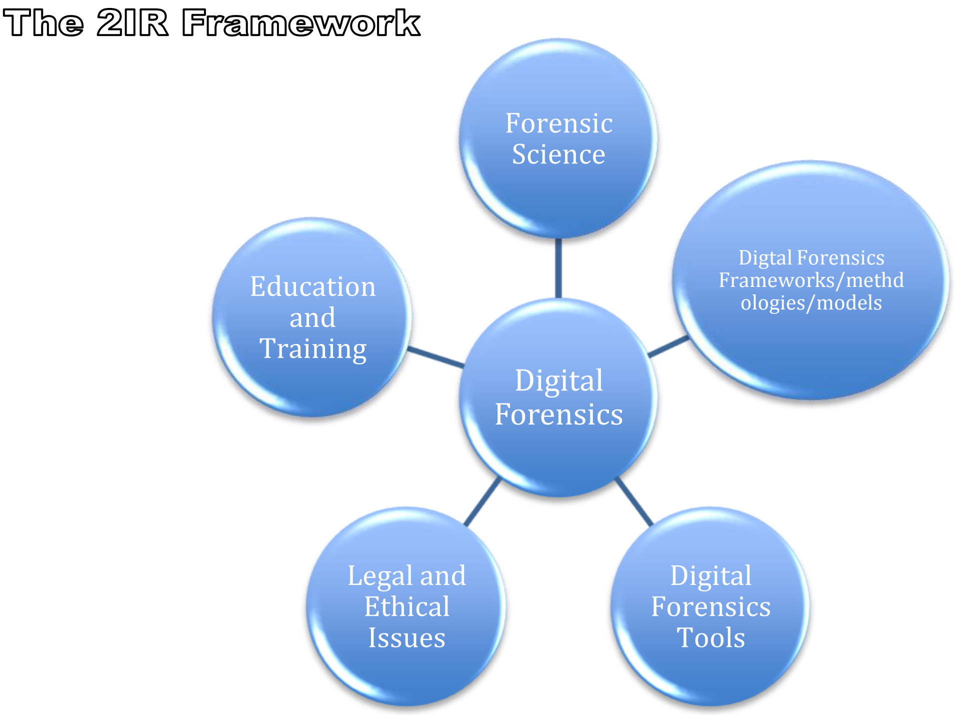


Figure 2.1 This figure outlines the various researched areas covered in the research and looks at how each component fits into the 2IR framework and methodology which emerges as a result.

2.1 Definition and context

Forensic Science has become popular in recent times, the popularity of Television shows involving forensics has propelled forensics into the forefront of the public view on solving of various types of crimes. The term forensic is defined basically as "science used for the purpose of law" (White 2010). The United Kingdom forensics science regulator defines it as "...any scientific and technical knowledge that is applied to the investigation of a crime and the evaluation of evidence to assist courts in resolving questions of fact in court" as noted by (White 2010). The origins of forensics dates back to the 6th century in Chinese history however it was not before the 18th century that the true types of forensic evidence as we know it today began to emerge. Forensic science has its roots in law and is sometimes referred to as forensics which itself means the application of science to law (Walker 2007). The terms forensics and forensic science are often used interchangeably and both have become popular in many disciplines. This could pose a problem if forensics is seen in its more narrow scope as dealing with physical evidence as opposed to forensics science which encapsulates a wider range of evidence including digital and engineering entities. Though forensics may be simply defined as the application of a scientific methodology in the legal system, (Casey 2004), outlines forensics as being "a characteristic of evidence that satisfies its suitability for admission as fact and its ability to persuade based on proof (or high statistical confidence)". He continues stating "Forensic science is the application of science to law and is ultimately defined by use in court". Staffordshire University Science department defines Forensic science as being "any science used for the purposes of the law" (SU 2012). Any field thus purporting to be an arm of forensics such as digital forensics must have as its main aim the collection, preservation and analysis of evidence to be presented in a court of law.

The word *sciences* in "forensics sciences" originally referred to engineering, which would be used for the identification and examination of structural designs, chemistry, for the identification and examination of explosives and biology (probably the most popular) for the identification and examination of blood (DNA). Forensic science may also be and has been applied in a number of fields including but not limited to meteorology, geology, anthropology and biology (White 2010). This 'forensic science net' has recently been expanded to include computer science for the identification and analysis of digital evidence. Forensic science is an investigative technique that involves using scientific methodology to uncover and gather evidence from the scenes of crime for use in the court of law. The popularity of this investigative technique is mainly due to its perceived reliability based on impartial scientific evidence that is deemed trustworthy. Forensic science occupies the positions of impartiality and trustworthiness in that: *it is possible to isolate evidence into unique components and the reconstruction of the incident scene to identify/create an intruder profile*. This therefore means that each piece of evidence can be looked at on its own merit. As a result it is considered trustworthy as forensics evidence is not easily manipulated. The reliability and trustworthiness is as a result of established standards in the forensics field over the years. Forensics has also become popular in the computer science field as digital devices are increasingly being used in the facilitating of crimes and thus there is need for standardization in the area to ensure the viability of the evidence produced.

The objectives of forensics, whatever the science, it is connected to is that which aids in confirming that a crime is committed and identifying who is responsible. An investigating officer with the help of additional personnel such as forensics practitioners will establish if a crime has been committed and if so who is responsible. To establish who is responsible enough evidence needs to be gathered to effect successful prosecution. (White 2010) notes that when the need for a forensic practitioner is established their duties may be identified as follows;

> *To examine material collected or submitted in order to provide information previously unknown of to corroborate information already available. To provide the results of any examination in a report that will enable the investigator to identify an offender or corroborate other evidence in order to facilitate the preparation of a case for presentation to court. To present a written and/or verbal evidence to court enabling it reach an appropriate decision regarding guilt or innocence.*

Forensic practitioners work along with law enforcement officers and investigators as a general rule to provide support regarding substantiating evidence in a case. This helps in validating evidence adding scientific proof. This also helps in the validation of evidence adding scientific proof to its weight. In many jurisdictions worldwide forensics practitioners are deemed to be independent witnesses for the courts. It is however critical that as such witnesses, forensics practitioners demonstrate a high level of integrity as well as a thorough knowledge of the scientific field they represent.

The forensics field places great emphasis on quality and is guided by the ISO standard 8402 1986, definition: “quality – The totality of features and characteristics of a product or service that bears on its ability to satisfy stated or implied need”. The practicing forensic scientist must satisfy this requirement through processing and delivery of service (forensics) to the customer (court) via an expert testimony or other forms of presentation. The quality of evidence produced from the digital forensics process is critical as it enhances the credibility of the digital evidence when presented in courts. The overall aim of this project is to develop a methodology that will produce quality digital evidence to be presented in a court of law. It has the reinforcements of the standards upon which it is based; that is the 2IR framework has its core genesis in the ISO standards 8402 along with the input of current forensics trend and designed policies.

Throughout jurisdictions worldwide there have been bodies formed to regulate the functions of forensic scientists and the general forensics practice. These groups facilitate the accreditation of labs, training and certification of practitioners, guidelines for practice and generally ensures some form of order to the practice. Organizations include, the forensic science regulator (UK) and the Forensics Science Society. The National Occupational Standards (NOS) of forensic science sets out the following professional guidelines for competence in forensic science.

Unit		Element	
1	Prepare to carry out examination	1.1	Determine case requirements
		1.2	Establish the integrity of items and Samples
		1.3	Inspect items and samples submitted For examination
2	Examine items and samples	2.1	Monitor and maintain integrity of Items and samples.
		2.2	Identify and recover potential Evidence.
		2.3	Determine examinations to be Undertaken.
		2.4	Carry out examinations
		2.5	Produce laboratory notes & records
3	Undertake specialized scene exam	3.1	Establish the requirements for the Investigation.
		3.2	Prepare to examine the scene of the

			Incident.
		3.3	Examine the scene of the incident.
		3.4	Carry out site surveys and test.
4.	Interpret findings	4.1	Collate results of examinations
		4.2	Interpret examination of findings
5.	Report Findings	5.1	Produce report
		5.2	Participate in pre trail consultation
		5.3	Present oral evidence to courts and Enquiries.

Table 1 Table of forensics process From www.crfp.org.uk

This table represents the general guidelines issued for the forensic sciences and some of these guidelines are general enough to be applicable to digital forensics. The type of evidence produced from the digital forensics process (digital evidence) is arguably different from other types of physical evidence encountered when dealing with other forensic sciences and thus these guidelines, though general enough to be applicable, they would need further amendments to adequately address the needs of the digital forensics field.

The alleged crime scene is the beginning of any investigation, the point from which any forensic examination will take place. The importance of capturing the crime scene in its truest form cannot be over estimated. (White 2010) emphasizes, “Get this bit wrong and the rest of the forensics process is nullified”. He continues stating that there is rarely a second chance to make good any mistakes that may have occurred in a forensic investigation. It must be noted that a crime/incident scene is not necessarily the place where a shooting, murder or robbery occurred. It refers to any location that may be connected to an incident which is of any interest to investigators. The crime scene as defined by the legal dictionary is “any location where a crime took place or any other location where evidence may be found”. This definition of a crime scene is particularly applicable to digital forensics as digital devices have become prevalent in the incident/crime scenes though not necessarily an implement used in the incident.

Crime scenes are usually examined by law enforcement officers or other officers of designated bodies. As a rule of law crime scenes are examined for a number of reasons. These reasons may include but are not limited to the following, identifying the person or persons involved in an incident. These persons may be the victim/s or perpetrator/s of the incident. Crime/Incident scenes are also examined or in some cases reexamined to ensure corroboration of incident reports and help to establish whether or not a crime actually occurred. There are times when the reports regarding an incident may be conflicting and examining/reexamining the scene of the incident may help to clarify issues surround the case. Carefully examining an incident scene can provide great insight about an incident and is an integral part of the general forensics process. This is also applicable to a computer crime/incident scene where devices have to be carefully examined and reexamined by personnel to establish exactly what happened. This is however not done at times and where it has been done has proved very valuable. [See case 10 – Florida vs Anthony - legal section 2.2.3]The prevalent use of computers and its related digital technologies have become increasingly popular (Nance et al, 2009). These devices are increasingly being used to assist in committing traditional crimes in new ways as well as to commit a whole new set of crimes (digital crimes). Digital/computer forensics has been developed to investigate and stem the increasing occurrence of such activities.

Digital Forensics is the branch of forensic science that has emerged to deal with the characteristics of legal evidence found in/using computers and other digital devices. Digital forensics is also referred to as computer forensics in some cases and may include sub divisions such as network forensics and mobile forensics. It is the way of collecting evidence, recovering data lost, determining how entry was made into a system, it also includes what was done and establishing a sequence of what happened involving the alleged device. This is an investigative technique used mainly to uncover and gather evidence on computer crimes such as hacking, computer related fraud and identity theft.

This increase in the use of digital devices in the last two decades has changed the scope of the traditional crime scene as well as created an additional type of crime scene. Digital devices are increasingly being used to commit crimes or as an accessory to a crime. Whereas the evidence from such scenes may be physical and easily accessible to crime scene officers others may exist in the digital realm proving to be more of a challenge. (Henry 2010) notes that the computer crime/incident scene exists in terms of the traces of actions performed on a computer that remain on the hard disk drive or removable media, a single line in an email header or even as entries in a server log file showing access to files or an email account. The digital crime scene consists of all digital devices and other related physical evidence that may exist. These digital devices may contain traces of digital footprints which may be reproduced into digital evidence to be used in courts. The extensive inclusion of digital evidence in the courts promotes the need for exploration of the legal context in which the digital forensics falls.

2.2 Legal Context

This section provides an overview of the legal context in which digital forensics falls. It highlights the different types and functions of science in courts, the evidence, the use and the guidelines that should be followed to ensure their admissibility in court. The section begins with a look at evidence in general and then proceeds to be more specific in looking at scientific evidence and then on to digital evidence.

Though there exists cases in which a digital forensics investigation may not end up in court the majority of the cases do end up there, whether as a criminal case or a civil one. To mitigate any legal dispute the court will endeavour to establish the necessary facts of case. These factual issues include, those on which the opposing parties agree, those whose existence can be used to prove or disapprove facts in issue known as circumstantial facts and those facts that must be proven in order for the appropriate law to be applied or for the evidence to be admitted into court. In a court proceeding the facts are proven by demonstrating evidence of the fact no other way.

A degree of certainty must be established by the trier/finder of the fact in order for the truth of the fact to be accepted (standard Proof). There are two major standards of proof, the criminal standards and the civil standard. The criminal standard as the name implies used in criminal proceedings where the finder of the fact must be persuaded beyond reasonable doubt to accept the truth of the fact. Civil standards used in civil proceedings on the other hand consider a fact to be true of the evidence for the fact prevail over the evidence against the fact.

The decision as whether or not a fact is true or false is for the most part never final. After a fact is proven it is assumed to be true. If additional evidence is revealed after that disproves the fact the finder/trier of the fact must change the original decision. Generally in a legal setting nothing is assumed about a fact in a case before it is proven despite some fact being assumed true from the initial stages. This is defined by the law in a case where an accused is assumed innocent until proven to be guilty. The party that carries the burden of proof has the duty of convincing the 'finder of the fact' into believing that the fact is true during the process of the fact being proved. The party that carries the burden of the proof is dependent of the case however it is usually borne by the party that declares the existence of the fact.

One of the features that is quite crucial to the legal context is the issue of admissibility. It has been found that in many cases where digital evidence would have been critical in bringing about convictions or the wrapping up of a case, the evidence has been deemed inadmissible because it fails to meet the stated criteria for admissibility, See Section 2.3.3 for applicable case.

2.2.1 Evidence and its admissibility to court proceedings.

Evidence is predominantly characterized by weight and relevance. The weight of the evidence is dependent on its believability and how convincing it is. Evidence deemed to be vague or indefinite will be of less weight than evidence that can be proven and is direct. How much the evidence is able to change the probability of the fact is essentially the weight of the evidence. Relevant evidence on the other hand is that evidence which has a relationship with the fact being proven. Evidence is relevant if it is directly or directly related to the fact to be determined and is able to advance the inquiry in making the existence of non existence of a fact more probable.

a) Admissibility

Evidence that is deemed admissible is that which a judge finds useful in proving the fact. In jurisdictions governed by common law evidence to be presented in courts must pass and admissibility test before it can it can be used. The specific admissibility test is dictated by law. The admissibility of the particular piece of evidence is dependent on how it is related to the fact to be proven as well as the type of dispute of which it is a part. If the evidence to be presented has no relation to the fact being proven it will be deemed inadmissible.

b) Types of evidence

Legal evidence is classified based on the type of fact it is to prove, its form, the laws that govern its use and the role it has in the case. Major classes of legal evidence includes:

Circumstantial, Direct, Hearsay, Documentary, Real, Testimonial, Expert Inculpatory and Exculpatory.

- Circumstantial evidence

Circumstantial evidence as defined as "…evidence that is drawn not from direct observation of a fact but from events or circumstances that surround it". Circumstantial evidence being that which suggest or infer the existence of the fact.

- Direct evidence

Direct evidence is not assumed or inferred it is directly related to the fact. According to the legal dictionary online direct evidence is "evidence that if believed, proves the existence of the fact in issue without inference or presumption". Direct evidence is concrete or firsthand evidence of the fact being proven.

- Documentary evidence

Documentary evidence includes any type of written evidence offered to support a fact that is being proven.

- Hearsay Evidence

Hearsay evidence is evidence that is not based on personal account of an event but on the account of another not made under oath. It is essentially second hand evidence. In hearsay, evidence is given not about what one saw or heard personally but about what one was told by someone who saw or heard.

- Expert evidence

Expert evidence is given with regards to a scientific or technical subject. An expert in a case would give testimony based on specialized formal training and /or experience in a particular field. This type of evidence is usually required when there are parts of a case that are outside the capabilities of the trier/finder of the fact. It is expected that an expert witness be qualified in the particular field in which they are to give evidence.

- Inculpatory and Exculpatory evidence

Inculpatory and exculpatory evidence are directly related to the function the evidence plays in a case. Inculpatory refers to evidence which can be used to establish the guilt of the person in question. It is that evidence that shows involvement in an act. Exculpatory evidence on the other hand is evidence that is used to establish the innocence of the person in question.

- Scientific Evidence

Forensic science according to (White 2010) 'forensics' refers to the application of science expertise in the form of knowledgebase and methodology within the court". It is the use of scientific techniques in a legal investigation producing evidence to be used in court. Science in used in court to establish particular fact which may be out of the trier of the facts' field of expertise. This suggests that where scientific evidence is gathered, the objective is for it to be used in legal proceedings. To ensure evidence is considered reliable when presented in courts, proper standards and procedures must be followed.

Prior to1975 courts in the United States relied on what was known as the "general acceptance" or Frye test to determine the validity of scientific evidence. This rule was based on a case in 1923 (Frye vs United States) as was set by the District of Columbia Court of Appeals. The rule stated if a particular scientific practice was generally accepted within a particular scientific community it could be accepted in court. The rule:

> *"While courts will go a long way in admitting expert testimony deduced from a well recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs".*

(Berstien 2008) suggests that the Frye test applied only to true scientific evidence and was mostly used in criminal cases. This case was a major impacting case in the United States it brought to the fore the fact that courts had the power to decide what should and should not be accepted as evidence. (Berstien 2008) continues stating that even though Frye may not have been often referenced in cases that involved scientific evidence the courts used "general acceptance" without citing the Frye rule.

In 1975 standards established by the Supreme Courts in the United States took effect essentially replacing the Frye rule. These were known as the federal rules of evidence (FRE) specifically Rule # 702 which now regulated the admissibility of evidence into the courtroom. This rule {#702} states:

> "*If scientific, technical, or other specialized knowledge will assist the trier of the fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods and (3) the witness has applied the principles and methods reliably to the facts of the case*".

From the 2IR in the educational facet of the framework, standard E1 states that the practitioner must have secure knowledge and understanding of the legal context in which they will function. This demonstrates the seamless link between the Federal Rules of evidence and the operational standards that have been put forward in this research. While this example is specifically relevant to the federal Rules of Evidence, other standards can be found to link with not only the federal Rules of Evidence but other existing principles and guidelines.

This rule which was updated in 2000 establishes the criteria for a witness to be considered an expert in a field. The stipulations set out in the Federal Rules of Evidence [FRE] (702) offsets and doubt that may have arisen from the Frye rule.

In developing a set of principles and/or a methodology it is important to be clear on the requirements of the domain in which the particular field falls. The purpose of having a digital forensics investigation is to find evidence that will lead to ascertain the perpetrators of a crime. Like other forensics fields digital forensics has a legal connotation to it. For digital evidence that is retrieved through the digital forensics process to be considered robust enough to stand up in court it must be able to satisfy legal testing criteria such as those outlined by Daubert and the Federal Rules of Evidence (FRE). To satisfy the ideals of Daubert criteria there are certain criteria that must be met:

1. Empirical testing: Referring to whether the theory or technique used is refutable, and/or testable.
2. Has the theory used has been subjected to peer review and has it been published?
3. What is the known/potential error rate?
4. Are there the existence and maintenance of standards and controls concerning its operation?
5. What is the degree to which the theory and technique is generally accepted by a relevant scientific community?

In 1993 there was a major ruling by the United states Supreme Courts on the case of William Daubert v Merrell Dow Pharmaceuticals. Despite having several scientific witnesses testify on his (Daubert) behalf the court decided that the evidence was not admissible. The ruling was as a result of the fact that the court thought the witnesses did not meet the standards set by the Federal Rules of Evidence. They stated the “general acceptance” (Frye) had been superseded by the Federal Rules of Evidence and thus general acceptance was not a necessary precondition to the admissibility of evidence under the Federal Rules of Evidence (FRE) (Daubert vs Merrell, 1993). The Daubert standards help to establish guidelines with regards to science and its use in law. In developing the framework of standards for digital forensics (which is the use of computer science in law) these standards had to be considered to ensure validity. The Daubert case established that expert witnesses must be trained in the area and that the procedures used must be replicable (other practitioners should be able to follow the same steps and arrive at the same results). This again links into the issue of trustworthiness. This assumption left the judge to make a decision as to whether or not the scientific testimony was reliable. This inadvertently extended the powers of judges to deal with and rule in cases involving scientific evidence. The judge could now (before a trial) rule on the admissibility of the scientific evidence and not only the credibility of the witness. (Carrier 2002) states that "the judge now has the burden of determining if the evidence is both relevant and reliable". (Rogers 2003) notes "This is a shift in power from the Frye test, where it was the scientific community that had to show that the science was true based on its acceptability in the community". With this new ruling from the Duabert case a hearing known as the "Daubert hearing" may occur before a trial allowing each side to present any science behind the evidence they need to be admitted in a case. This evidence must satisfy the questions as presented above.

2.2.2 Digital Evidence

Forensics is the application of science to legal issues. (Saferstien 2009) defines forensics as "the application of science to the detection, examination and presentation of evidence in legal proceedings". There are fields that apply forensics science. These include but are not limited to physics, chemistry, toxicology and accounting. These fields all provide a physical context by which to understand the evidence. Digital evidence on the other hand exists in a different context to these other forms of evidence. Digital evidence exists 'digitally' in the form of electronic pulses, zeros and ones. This difference means that its acquisition, analysis, interpretation and presentation in seen differently in court.

Digital evidence that may be recovered from the 'scenes' of these crimes may be defined as "any data stored or transmitted using a computer that support or refute a theory of how an offence occurred or that address critical elements of the offence such as intent or alibi", (Casey 2004). This evidence is recovered through the digital forensic process.

Despite being in use for over a decade there are significant problems facing the digital industry with regard to Computer/digital forensics. Whereas there is the growing need to secure data and information that reside digitally and there are a number of threats to this security there are issues regarding how digital/ computer forensics is carried out as well as the acceptance of digital evidence in courts. The 2IR developments presented in this project puts forward principles for the acquisition of digital evidence which makes the evidence more readily acceptable in court. For example LI$^{(2)(1)}$ purports that the use of cryptographic hashes to ensure that results are duplicable which speaks to its authenticity. (Meyers and Rodgers 2004) writes, "Search and seizure of digital evidence is often the first process that is disputed. If it can be shown that this step was not completed properly, the defense or prosecution's evidence may not be admitted". This statement also highlights the need for a defined and standard set of procedures to be used in the digital forensic process.

The fundamentals of any digitally related criminal activity is "digital evidence". This evidence is acquired through the digital forensic process, which involves collecting, preserving and presenting this evidence. This process as described may vary between investigators despite the various legislations in place as there is currently no universal definition for digital evidence. Additionally there is no existing foundation research or substantial body of academic literature regarding digital evidence. (Kessler 2010) Digital evidence is unique in a number of ways based mainly on the form it takes which is not necessarily a physical one. (Mercer 2004) notes "if someone opened a digital storage device they would see no letters, numbers or pictures on it". The very nature of the data highlights the need for a digital forensic investigator to be vigilant in carrying out their duties as well as be appropriately prepared for the duty.

The term Digital Evidence is also defined as, "Encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator" (Casey 2004). The same term may also be defined to be, any data or information found to have been stored or transmitted in a digital form that may be used in court. This type of evidence has become increasingly popular in recent years with the prevalence of computer technology, and courts have begun to accept electronic based evidence for use in various types of cases.

As with other types of forensic evidence proper standards and procedures must be followed to be admissible and considered reliable in a court of law. Over time a number of courts have found it necessary to question the reliability of such digital evidence when presented. [See cases section – Section 2.2.3] This concern has been highlighted by some practitioners with the lack of standardization in the acquisition of digital evidence (i.e. Computer forensic methodologies) being blamed. (Casey 2004) states, "Digital investigators do not have a systematic method for stating the certainty they are placing in the digital evidence that they are using to reach their conclusions". The methodologies and tools used by digital forensic investigators worldwide have been variable and there is no one internationally accepted benchmark that is used to acquire digital evidence through the digital forensics process. Casey continues, "This lack of formalization makes it more difficult for courts and other decision makers to assess the reliability of digital evidence and the strength of the digital investigators' conclusions". This issue is further highlighted by (Fulbright and Jaworski 2006) where they state, "The number one problem in current litigation is the preservation and production of digital evidence". There are a number of tools, models, methodologies, guidelines and frameworks available to carry out the digital forensics process however there is no standardized format in place.

The problem of standardization in the area of Computer forensics has been an issue from the conceptual stages and still faces major challenges when digital evidence is to be presented in court. "Because computer forensics is a new discipline, there is little standardization and consistency across courts and industry"(US CERT, 2008). One major step to overcoming these challenges for the different agencies and practitioners to adhere to a defined set of standards and operating procedures such as is suggested in the 2IR designs.

Sartin, Managing director of Cybertrust), in an interview with SCmagazine for Security Professionals notes that there is still much more to be done where digital evidence is acquired through computer forensic is concerned. He points out that, "There are two things missing: a single commonly accepted standard and uniform code of working…. Quality of service across computer forensic providers varies dramatically …" (Chaikin 2007) sums up the need for standardization within the sector when he noted, "…there is an absence of generally recognized standards of best practice in digital evidence forensic procedures, and a lack of adequate training of forensic examiners". He made a very valuable point when he continues his argument, "errors in analysis and interpretation of digital evidence are more likely where there is no standard procedure for collecting, preserving and analyzing digital evidence". These are some of the combining factors that facilitate the challenges facing the acceptance of digital evidence in a court of law. Digital forensics is defined by United States Computer Emergency Readiness Team as being "the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law". (US – Cert, 2008,) The Scientific Working Group on Digital Evidence (SWGDE) defines digital evidence to be "any information of probative values that is either stored or transmitted in digital form". Computer forensics or forensic computing as it was initially referred to dates back as far as the early 1980s. This was just about the beginning of the extensive use of personal computers. As personal computing became more popular so did the crimes involving computers and the awareness of the need of disciplines such as Computer/Digital Forensics. The actual term computer forensics came about in 1991 at the first training session of International Association for Computers and Information Systems (IACIS). In 1993 the first (recorded) international conference on computing evidence was held with the formation of the International Organization on Computer Evidence (IOCE) two years later in 1995. Since then there has been a number of organizations formed to deal with digital forensics and the digital evidence acquired form the process by different organizations and countries.

Different groups have been formed in an attempt to address the issues involved and surrounding digital forensics, the fact that today's society is becoming (and will continue to do so) more and more dependent on digital devices the quality of digital evidence forms an integral part of an increasing number of court cases and thus its importance cannot be over stated. The mere quantity of digital information that may exist on any computer, other digital device or network presents the digital forensic investigator with a myriad of challenges

Digital evidence present challenges, as it is inherently different from other types of evidence that may be acquired from forensic investigations in other fields. (Chaikin 2007) notes "Digital evidence is different from evidence that has been created, stored, transferred and reproduced from non digital formats". The main differences include the fact that digital evidence can be easily reproduced and manipulated by investigators and others involved maliciously or accidentally. The difference in the nature of digital evidence is supported by (Casey 2004) where he notes that the very nature of digital evidence (referring to its intangibility), is distinctly contrasting to the features of evidence used in other disciplines. An important point to note which has been argued in some regions is that some definitions of digital evidence propose that this type of evidence includes any information that may have been stored or transmitted on any digital device not just limited to computers and associated networks but mobile devices, audio, video and others. The nature of digital evidence is therefore not limited to a particular format, which in itself can present a problem. The diversity of formats is catered to by the flexibility of the standards proposed by this research. (Chaikin 2007) notes that, "Digital objects bear less evidence of authorship, provenance, originality and other commonly accepted attributes than do analog objects". These characteristics leave themselves open to doubt and thus there must be standardized way of acquiring digital evidence to ensure validity.

(Kessler 2010) supports this point noting that the differences in digital evidence and physical evidence have direct implications for the practice of digital forensics. There are also legal issues associated with the acquisition and analysis of the digital evidence produced from the digital forensics process. There is the integral issue of a search warrant and its scope given the nature of digital devices and their connectivity. (Kerr 2005) notes, inconsistencies in Rule 41 of the Federal Rules of Criminal Procedure in the US which governs search warrants (US Courts, 2008). This rule 41 states that search warrants should be narrow in scope, clearly identify a specific time and place for search, and specify the evidence that is being sought. Where physical evidence is concerned this particularly easy to do however the nature of digital evidence makes this a bit more challenging. (Kerr 2005) indicates that with digital evidence the entire store of digital data is seized at the search warrant location, while the actual search of the hard drives and other media to determine what information has probative value typically occurs at a specialized lab well after the warrant has been served. (Kenneally and Brown 2005) via (Kessler 2010) states, "in addition the search of digital evidence is often complicated by large volumes of digital evidence (due to a growing disk drive capacity) that is seized”. To reduce the challenges faced by digital forensics there are a lot of improvements needed in the field. One way to do this is to start by standardizing how the process is carried out.

There have been a number of arguments for and against standards in computer forensics. This, despite the fact that the need for standards was identified as far back as 2001 during the first Digital Forensic Workshop held. Since then there has been very little progress in this regard, which is proving to be restricting where growth and expansion of the field is concerned. The judgments resulting on a number of cases that involved the use of digital evidence (Mason 2013) suggest there needs to be some standards by which digital forensic practitioners abide to help in ensuring that the evidence acquired is valid in court. Technology is ever changing and thus the digital forensics field is very dynamic however standards can be developed provided they are flexible enough to adjust to the constantly developing technologies. Carrier and Spafford (Carrier and Spafford 2003) in an article entitled “An event based digital forensics” argued that developed standards needed to be “flexible enough so that it can support future technologies and different types of incidents”. Such a development is exactly what is needed namely a set of standards which fulfills such a criteria that is flexible enough to be able to serve as an international benchmark for digital forensic practitioners. Flexible enough to be used in different jurisdictions as well as for the different types of digitally related forensics namely mobile, cloud etc. This work presents a set of policies and guidelines that are able to do this.

2.2.3 Use of Digital evidence in courts

Decision in cases involving digital evidence rest mainly on the judge’s and/or jury’s understanding of the technology, digital evidence as well as the ability and reliability of the expert witness (Mason 2008), (Kessler 2010). The following examples are some of the cases reviewed by the researcher in preparing this research. These cases highlight some of the issues facing the courts with regards to digital evidence. In a society driven by technology cases of different origins now involve the use of digital evidence and courts are now faced with the tasks of making decision based on the origin of the evidence, the applicable laws, the reliability of the expert witnesses and the process used to acquire and preserve the evidence. By recognizing the deficits within the field, the construction of a set of standards is a timely response to an area of need in the digital forensics field.

Case 1

Debtor American Express Travel Related Services Company, Inc v Vee Vinhee (2005)

American Express (AMEX) brought a case against Vinhee for more than 21,000USD in outstanding bills. At an initial hearing, the bankruptcy court disallowed AMEX's use of electronic records as their best evidence of the amount owed. This decision, based on the FRE Rule as discussed above, defines hearsay exception for records of regularly conducted activity (US Courts, 2008).

> *The rule states that business records can be introduced as evidence if it can be shown that the records were made at or near the time the activity occurred, that the records were created and maintained pursuant to regularly conducted business activity: the source, method or circumstances of preparation of the records can be shown to be trustworthy. These records must be maintained by a records custodian and must be shown to be authentic and accurate. (Mason 2008)*

In the case of Vinhee the records custodian form AMEX testified that their records had met the requirements of all the tests. They however offered duplicate copies of the records that had been produced from an electronic backup as evidence.

American Express, in this case, contended that the courts take notice of the "accuracy and reliability" of their computers when ascertaining the authenticity of their billing statements. The courts rejected this for a number of reasons that included:

1. Just asserting that their procedures for maintaining electronic records were designed to ensure accurate records and identify any errors in records was not enough to prove authenticity of the digital evidence.
2. The statement given by their expert witness was considered vague and assuming, stating "there is no way that computers changes numbers". The witness was deemed unpersuasive.

The trial court ruled, the declaration was deficient as to basic foundational requirements for admission of electronic records, noting particularly the need to show the accuracy of the computer in the retention and retrieval of the information at issue. The court stated that because the records were stored electronically they would require additional information to prove authenticity and value as evidence. Later the court then found the AMEX custodian was not qualified to adequately answer questions on the same basic hardware, software and databases with which the electronic documents had be created and stored. The Judge suggested that AMEX could not authenticate the billing records and thus was not allowed to enter them as evidence.

This case highlighted the fact that authenticity of digital evidence requires evidence from qualified witnesses not just experienced practitioners. It also highlighted the need for maintenance of a reliable chain of custody to increase the validity and robustness of evidence acquired. The 2IR designs were developed with such considerations in mind. The assist the digital forensics process with the issue of maintaining a reliable chain of custody and observation of the legal facet of the field. These considerations improve the robustness and reliability of the digital evidence acquired when presented in court.

Case 2

Zubulake v UBS Warburg (2003) [http://lawschool.courtroomview.com]

This case involved an employee Laura Zubulake accusing the company of gender discrimination and wrongful termination. In this case the Plaintiff sought access to electronically stored information in the form of emails stored and archived by the Defendants.

Several important factors were highlighted in this case with respect to digital evidence. The ruling which was not in the company's favor suggests that they would have benefitted had they preserved evidence from the initial stages of the case. (Maynes and Downing 2009) states, "The duty to preserve is not just limited to evidence that may be admissible in court but to anything that seems likely to lead to the discovery of other admissible evidence". This case was deemed to be an important case in the development of the field as it highlighted the strength of digital evidence in courts, cases of varying origin as well as and the need to ensure preservation of evidence and chain of custody.

The increase in the use of digital evidence in courts has resulted in the need for formalization of the digital forensics field which is the process used to acquire digital evidence. To ensure the increased strength and viability of the digital evidence the digital forensics process needs to be acquired through a process guided by crafted principles and standards such as those presented in the 2IR designs in this research.

Case 3

Coleman Holdings Inc v Morgan Stanley.(2005) http://www.ediscoverylaw.com

In this case digital evidence relevant to the case was not presented despite being identified. Additionally the company in question (Morgan Stanley) used "inappropriate" tools to acquire digital evidence. (Manes and Downing 2009) argue, "Morgan Stanley was found to have relied on flawed software written by its in house Information Technology department". The judgment also indicated that Morgan Stanley used "flawed" dates range in their search for emails while also failing to capture attachments to emails.

This case clearly highlights the necessity for a standard policy to be established in the industry with regard to the identification, preservation and presentation of digital evidence acquired through the digital forensic process. It also highlights areas presented in chapter five for the need of qualified digital forensic personnel and approved tools to carry out the procedure and standardization of the process.

Case 4

As alluded to in the body of this thesis it is a legal requirement to ensure that: (1) a warrant (i.e. Legal permission) is received before attempting to search a suspect device. (2) Analyze data that relevant to the particular case being investigated (only).

United States v Carey (1998) [http://laws.findlaw/10th/983077.htm]

In this case Carey was suspected to be involved in possession of cocaine. A warrant was granted to arrest Carey. During the arrest, Officers noticed other items in the apartment that may have been related to the case. They negotiated with Carey and he consented to them searching the apartment (this was then signed and made a legal document). Armed with this document they searched and found a number of incriminating evidence including two computers believed to have contained evidence of drug dealing.

Investigators obtained another warrant that authorized them to search for files containing evidence pertaining to the sale and distribution of controlled substances. During this search the investigators found files with titles that contained child pornography. After hours of searching through the child pornography files they charged Mr. Carey with one count of child pornography.

In an appeal, Mr. Carey challenged that the child pornography was not admissible in court because the files were found in a "warrantless" search. Though the prosecutors argued that the initial warrant authorized detectives to search any file as they could have contained information to drug deals and that the pornography came into view during that search the court ruled that the detective's search exceeded the scope of the warrant.

The use of the 2IR framework and methodology negates the occurrence of such issues as identified in this case. These designs dictate the importance of acquiring a search warrant before activities of the investigation begins. The framework outlines that the warrant should cover all the areas of the investigation. The investigator should not deviate from the specifications of the warrant. If needed the practitioner should request another.

Case 5

United States v Benedict [http://www.cybercrime.gov/]

This particular case indicates how critical it is to take great care when acquiring and preserving digital evidence. Benedict was accused of possessing child pornography. This was found on a tape he had exchanged with an individual who had previously been convicted of possession of child pornography and sexual assault of a minor. Benedict claimed he was exchanging games and did not realize the tape contained files of such nature.

He initially pleaded guilty but then changed his plea when he realized that there were issues concerning the "digital evidence related to his case.

Issue 1 - Storage – The computer and disk containing the digital evidence for the case was stored in a post office that experienced flooding.

Issue 2 – Acquiring evidence – When the device belonging to the other individual with whom the tapes were exchanged was seized the investigator copied the data from the tapes onto the computer.

The Investigator also installed the forensic software to be used in the investigation on to the suspect computer. This resulted in the state of the device being altered while in police custody.

Digital evidence is sensitive by nature of its form and thus care must be taken by digital forensic investigators to ensure that data/files on the suspect device/computer is not altered in any way while in their custody. This is one such case highlighting the need for a set of procedures and standards to acquire digital evidence. This research satisfies the need for such guidelines and principles. It presents a framework of standards governing the digital forensics process and by extension other areas of the field such as education.

Case 6

Aston Investments v OJSC Russian Aluminum (2006) [http://www.deaeslr.org/2008.html]
Overview

Aston Investments accused OJSC Russian Aluminum of hacking into their computer systems in London and viewing confidential and privileged information related to litigation that they were both engaged in.

- Upon investigation it was found that hidden spyware in the form of a "key logger" was installed on Aston Investments systems. It was also found that a number of attempts were made to access these systems form varying IP addresses (one of these IP addresses belonged to OJSC). These attempts were revealed to have been successful.

Despite this overwhelming digital evidence problems existed with the case for Aston Investments. The digital evidence was not properly preserved as the internal IT Department (with no particular Computer/Digital Forensics specialist) in an attempt to prevent further unauthorized access to their systems had altered the evidence that could have proven useful.

Upon discovery or being alerted of a digital crime it is important that careful steps are made not to distort whatever evidence may exist.

Digital evidence acquired through the digital/computer forensic process can prove useful in a case when properly carried out with all legal aspects carefully followed and documentation consistently done. Proper preservation and documentation of the process helps to maintain the integrity of digital evidence acquired as highlighted by this research and the presentation of findings and outputs of the 2IR Framework and Methodology.

Case 7

Four seasons v Consorcio Bar (2003) [http://www.laws.lp.findlaws.com]

Action was brought against the defendant on this case for accessing the plaintiff's network, downloading confidential data, deleting files and overwriting data before the computer was handed over to the digital forensic investigators for examination.

The plaintiff hired a Computer/digital forensic investigator to examine the computer investigating the above-mentioned crime. After careful examination and presentation to the courts it was ruled that the defendant had indeed acquired electronic information (confidential customer information) illegally.

The investigation had revealed intrusion, existence of false evidence, deleted files and timely intrusion of network facilities. As an investigator like any other a digital forensics practitioner must be ethical in conducting the job despite who the employer might be. The 2IR framework of standards produced by this research looks in depth at the ethical facet of the digital forensic field providing as set of standards that specifically addresses that area. See Chapter 5 Section 2

Case 8

R v Cochrane (1993) [http://www.hse.gov.uk/enforce/Enforcementguide]

After having some money mistakenly credited to his account Cochrane used his cash card to withdraw this money. He was subsequently charged for theft.

The prosecutions cases did not hold due to issues with the digital evidence.

Despite the fact that information was relayed from the cash point to the branch computer which retained this information before transmission to the mainframe the court found that the prosecution's witnesses had no knowledge of the workings of the mainframe computer and thus was not able to adequately convince the court that is was working correctly at the time of the incident. Thus the till rolls and other digitally related evidence was deemed inadequate.

The need for trained personnel in the field has become even more important as the use of digital evidence becomes predominant in court cases. The work presented by this research includes a curriculum for the education and training of digital forensics professional addressing the need for trained personnel in the field and helping to ensure that all personnel can prepare robust evidence to be used in court.

Case 9

United States v Councilman (2004)

In this case a criminal charge was laid against the defendant Branford C. Councilman for the interception of emails while they were in temporary storage en route to their final destination. Councilman worked for a company Interloc Inc. that specialized in rare and out of print books, additionally they provided and email service offering customers an email address on their domain. Councilman being in-charge of the email service and subscriptions list directed the company's system administrator to configure the email server enabling it to intercept all incoming email messages from Amazon.com domain to customers and make copies of them prior to the individuals receiving their messages. Councilman was then charged with conspiring to violate the wiretap act (1986) that addresses the issue of monitoring real time communication in transit. According to (Casey 2011), email that is stored prior to being read is considered to be in transit whereas email that is stored after being read has a lower level of protection.

Councilman was however not charged for any violation under the Stored communications act (1986) that protects email that is stored prior to being read by the recipient. The judge cited that the email was protected by the wiretap act (1986) only while traversing the network and not when stored on computers during transit and delivery. Initially Councilman was indicted for intercepting emails as a violation of the wiretap act (1986) however the district court disagree and dismissed the indictment. On the other hand the first circuit court of appeals with a divided panel affirmed the ruling of the lower court (US vs. Councilman 2004) while a full panel reversed the previous ruling in 2005 (US vs. Councilman 2005). This case highlights some of the issues faced by stakeholders with regards digital evidence in courts and the need for standardized protocols and laws to address them. The 2IR framework and methodology were developed after careful exploration of the different related laws from different jurisdictions (as presented in section 5.2) thus the resulting 2IR application is guided by legal principles.

Case 10

State of Florida vs. Case Anthony (2011) http://lawrecord.com/2011/08/11/the-case-of-casey-anthony-defending-the-american-jury-system/

In this case the defendant Casey Anthony was accused of premeditated murder of her daughter Caylee. Caylee who was two years at the time was reported missing by her maternal grandmother Cindy who indicated that she had not seen Caylee for 31 days and that her daughters car smelt like a dead body had been inside it. Casey has reportedly given her a number of explanations for Caylee's whereabouts before finally telling her she had not seen her for weeks. She also told the detectives several stories regarding the disappearance of her child. Caylee's remains were eventually found and Casey stood trial. The trial lasted six weeks.

In this case a recovered Firefox 2 history from the unallocated space in the hard drive on Casey's computer became the highlight of the case regarding arguments of premeditation as presented by the state. Throughout the course of the trial, there were two different reports tendered by members of the Orange County Sheriff Department. One that was created using NetAnalysis dated August 2008 and the other created using CacheBack Version 2.8 RC2 in December 2009. A discrepancy arose from the trial with these two reports regarding visit counts where the expert witness (Digital Forensics Practitioner) for the state indicated that

Casey had conducted extensive computer searches on the word ‘Chloroform’ with 84 visits at chloroform.htm and at sci-spot.com actions that would suggest planned murder, a report compiled from use of the CacheBack digital forensics tool. However the report from the NetAnalysis tool suggested only one search count for the same search terms. As a result of this discrepancy a lot of doubt hung over the evidence which was been seen by some to be one of the deciding issues in the no guilty verdict. This case clearly highlights the need for several things with regards to the digital forensics field:

1. Standardization in the conducting of Digital Forensics examinations. A standards set of procedures that can be replicated by any digital forensics practitioner producing the same results. An integrated methodology that can be replicated by digital forensics practitioners from varying backgrounds helps to alleviate such issues as highlighted in this case.
2. A bench mark set of tools that is employed for use in the field worldwide not just any tool developed by someone with the deemed technical expertise. The developed 2IR Methodology presented in this work includes the recommendation of particular tools both commercial and open source.
3. The sensitive issue of educational background is key to the development of any field whether it be mainly theoretical or practical. Law enforcement officers, Information technology/Computer Science personnel and Legal personnel must be made to meet particular basic educational requirements. The research outputs include a programme of studies for persons wishing to pursue digital forensics as a profession at different levels. These being inclusive of certificate, undergraduate and postgraduate work with a suggested body of study.
4. The issue of ethics also arose, after the incident one of the practitioners involved who also discovered a flaw in one of the software tool used (developed by him) John Bradley, inquired of the Sergeant from the Orange County Sheriff’s department about the discrepancy in the findings. The officer allegedly knew of the discrepancy long before the trial but made no attempts to verify or validate.

The main area of concern in some communities is directly related to the admissibility of digital evidence in courts internationally. The evolution of digital evidence has had a significant impact on court proceedings.

With the continued extensive use of technological devices in all aspects of life digital evidence has become more frequent in its use with traditional cases. Drug trafficking cases, murders, fraud and others now involve having some information/data on a digital device that is needed in the presentation of a case.

There may be the general acceptance of the importance and relevance of digital evidence in courtrooms worldwide however the means by which this evidence is acquired still requires some consistency and uniformity. (Kessler 2010) notes that some Judges hold digital evidence as having limited value because of the difficulty in authenticating its original source. There is also the concern of court personnel's comfort level with computers and computer science issues. This raises the question of education as it relates to different personnel connected to any given case. There is a need for education on the part of legal personnel, Judges, and lawyers as well as the court staff. This group of persons should be able to comprehend what is being delivered by the expert witness as well as basic knowledge of the digital forensics process. Digital forensics is often carried out by technical or Information Technology personnel from a particular organization or by a technically inclined police officer. To ensure the development of the digital forensics field and greater acceptance of digital evidence barring reliability issues specific persons in this field should be appropriately trained to carry out a digital forensics investigation. This is because as alluded to before, the nature of digital evidence differs from that of physical evidence as well as the fact that digital forensics, the process used to acquire this evidence, encompasses at least four different fields. This work lays out a framework coving the four core facets of the field (legal, technical, educational, ethical) ensuring that all are covered while the methodology is in use.

There are also concerns along with the acceptance of digital evidence in courts about the education and qualifications of those collecting and presenting this evidence. There seems to be no uniform way in which the data is collected, the tools used and presentation of the evidence. Rogers and Siegfried (2004) also suggest this stating, "there is very little evidence of any unified strategy being developed in the field of digital forensics". This, coupled with the fact that it is a relatively new field has made digital forensics very suspect to the onlooker. There is the additional concern that digital forensics has been allowed to become widespread (development of tools, ad hoc training programmes, etc) without any baseline research guiding its development. A point highlighted by (Peisert et al 2008) "...computer forensics evidence has matured without foundational research to identify broad scientific standards, and without underlying science to support its use as evidence". Activities vary among universities, organizations as well as organizations and individuals involved in digital forensics. Such a diverse approach to development in the field presents issues of inconsistency among practitioners in the practice and presentation of the evidence acquired. These inconsistencies present problems where the evidence acquired end up in a court of law.

2.2.4 Applicable Laws

Governments worldwide are responsible for imposing regulations and controlling activities within the geographical confines of the borders of their countries. These governments are not usually concerned with the laws and regulations of other countries unless there are issues that require multinational cooperation that will in-turn be of benefit their country or impact it in some way. The expanding use of the Internet has brought to the fore some significant concerns with regards to borders or the lack thereof. The Internet is arguably radically different in nature from other developments encountered in the modern times as it impacts almost every nation of the world driving new and traditional activities. Added to this fact, no individual or country can claim governance of the Internet, which has no physical geographical borders. (Kohl 1999) notes, “The design of the World Wide Web allows one to enter multiple jurisdictions simultaneously, without targeting any particular jurisdiction and without leaving a physical trace in any of them”. With the advent of an increase in criminal activity online the nature of the internet presents a number of security and forensics issues. Criminals are now facilitated by the provision of more sophisticated technology and methods of committing traditional crimes (such as accounting fraud) with an additional level of cloaking has resulted in the development Computer related laws to govern the storage and manipulation of data as well as the use of computers. (Lee et al. 2001) indicates, “Within the past few years a new class of crime has become more prevalent, that is, crimes committed within electronic or digital domains, particularly in cyberspace”. Governments and various law makers worldwide have now realized that traditional laws and investigative methods are not necessarily effective in solving computer/cyber related crimes and have developed laws to address such. These laws must be considered with regards to digital evidence and the manipulation of digital evidence. Different Jurisdictions have laws and acts in place albeit by different names that address information technology related issues such as privacy, data protection, computer misuse and abuse. Research has found that existing guidelines and principles addressing the digital forensics process do not specifically address these laws. An example is the fact that the ACPO guidelines used in the United Kingdom do not specifically address laws such as the Data Protection Act. Some acts/laws related to technology found common in the jurisdictions looked at include;

The Data Protection Acts this act governs the protection of peoples personal data (Any data about a living Identifiable individual)in the countries that they have been developed. It aims to protect peoples fundamental rights and freedoms and their right to privacy in the processing of personal data. The Law mainly applies to organisations holding peoples' data/information. The act stipulates the protection of all personal data, it aims to protect peoples fundamental rights and freedoms and a digital forensics practitioner needs to be aware of any personal data that may be encountered throughout the digital forensics process. Knowledge of any data that is being held by the organisation or any personal data of any individual on a machine being investigated should be made known before the process actually begins as it could impact the investigation.

The Computer Misuse Act Developed to tackle problems caused by access to digital devices without authorization, this act governs the unauthorized access to a computer with intention to break, change or copy files. It dictates the following offences; unauthorized access to computer material, unauthorized access with intent to commit or facilitate a crime, unauthorized modification of computer material as well making, supplying or obtaining anything which can be used in computer misuse offences. While it is likely that the rationale for a digital forensics request lies within the remit of breaching this law the practitioner needs to ensure that he/she does not breach it as well.

The Computer Fraud and abuse acts This act was developed to reduce unauthorized access to computers and related devices. It makes it illegal to access computers without being authorized. It specifically addresses acts such as computer espionage, computer trespassing, computer fraud and password trafficking. Despite the fact that the practitioner needs to be cognizant of this law throughout the investigation this law is especially applicable to the investigation phase of the digital forensic investigation as it makes it illegal to access any computer or related device without permission and thus before actual examination of any computer related device takes place the practitioner must ensure that there is express permission to do so by the relevant stakeholder.

Intellectual Property Laws Intellectual property is a legal concept common in jurisdictions around the world referring to the creations of the mind for which exclusive rights are recognized. According to (Lloyd 2004) this law protects the rights of those who create original works. The purpose of Intellectual property laws is to encourage the development of new technologies, and new inventions in turn promoting economic growth.

Copyright Laws Copyright laws are also common in jurisdictions around the world they protect the expressive arts. Copyright laws give owners exclusive rights to produce their work, publicly display or perform their work and create derivative works. Such laws are important in the conducting of the digital forensics process as whereas breach of this act may not be what is being investigated there is possibility of breaching on the part of the practitioner during the Investigation.

Trademark Laws These protect the names and identifying marks of companies along with products. A trademark makes it easy for consumers to distinguish between products. Trademarks are common to jurisdiction worldwide.

Patent Laws Patents are of three types Utility, Design and Plant. A patent protects an invention from being made, sold or used by another person for a specific period of time. Utility patents protect inventions that have a specific function such as machines and technology. Patent laws or their variations are common in jurisdictions internationally.

Privacy Laws These are laws that deal with the regulation of personal information which may be collected by governments, public and private organizations. These laws also govern their access, retrieval storage and use. Privacy laws found in jurisdictions of large countries such as Australia, Brazil, UK, US, Canada, and India among others may be classified based on specific information. There are laws relating to general privacy, health privacy, financial privacy, online privacy, communication privacy, and information privacy. Privacy Laws are integral to be considered by any digital forensics practitioner considering conducting a digital forensics investigation.

Cybercrime laws These laws are developed to address legal issues related to online interactions and use of the internet within particular jurisdictions. They criminalise offences such as illegal access, data interference, device misuse, cybersquatting, computer fraud and spam among other offences. The cyber law in some developing countries compliment traditional criminal acts such as fraud and pornography.

Search and Seizure: Laws regarding searching and seizing evidence is paramount in the digital forensics process. These laws for the most part come with evidence acts which dictate that practitioners/officers must obtain legal authorisation before entering a property with the objective of collecting evidence. This authorization to search a location and seize property is common in several jurisdictions including that of the United States, CARICOM countries and the United Kingdom.

International Cyber crime law/treaty - these are guidance notes developed at the council of Europe including that of the United States, CARICOM countries and the United Kingdom. It dictates that practitioners of digital forensics use evidence to help track and apprehend cyber criminals across borders. (Steven Masey 2013) notes that these are guidelines and they do just that. These guidelines guide a practitioner gathering digital evidence in maintaining a particular standard as set out by the treaty they do not specify other legal issues that may be associated with the process.

There have been laws passed in a number of countries that address cyber related crimes. The nature of the Internet, that of existing without borders presents challenges with regards to jurisdiction. Countries/jurisdictions differ in how they treat different crimes and evidence as well as the rights of an accused based on their legal systems, culture/traditions and the role of their judiciary. Organizations such as InterPol, Europol, The European Union and The United Nations are seeking to address the issue of the international scope of cyber crimes with lack of geographical borders.

2.3 Frameworks/models/methodologies

A framework is defined to be “A Structure for supporting something else”. The Oxford Dictionary defines it as being “In extended use: an essential or underlying structure; a provisional design, an outline; a conceptual scheme or system”. A Methodology is “**a** method or body of methods used in a particular field of study or activity”. A model is “a thing used as an example to follow or imitate”. This chapter presents a review of key literature about issues and developments surrounding digital forensics and the digital evidence produced from the process. The literature reviewed looks at the prevalence of digital evidence in courts, the legal foundation of forensics and the acceptance of digital evidence in courts. Included in this review is literature regarding different models, methodologies and frameworks (terms used interchangeably in the field) developed for the digital forensics process. The references made to methodology and framework is especially significant in this work as it presents a twofold system with there being a framework of principles and a step by step methodology to carrying out the specific process. Both designs considered to be valuable to the development of the digital forensics field.

At the beginning of this research in 2010 a literature search was conducted into existing digital forensics models, methodologies, frameworks and standards. This was to identify any existing patterns and issues within the field. This literature search utilised several, computer science, legal, and general education databases. These included Lexis Nexis libraries, Association of Computing Machinery (ACM) Digital Library, Institute of Electrical and Electronics Engineers (IEEE) Computer Society Digital Library and Google Scholar. These database as well as Elsevier and Journal of Digital Forensics Security and Law (JDFSL) were again reviewed during the summer of 2012. Articles were found on Digital Evidence, Digital forensics models, methodologies and frameworks the latter three terms being used interchangeably. Digital/Computer Forensics has fairly few dedicated journals to the field. To date the researcher has examined issues of Digital Investigations, Journal of Digital Forensics Practice, International Journal of Digital Evidence, the proceedings of Digital Forensics Workshops and Advances in Digital forensics. Of all the journals and proceedings reviewed only one had papers specifically related to standards in Digital forensics and this was published in 2011. This paper, an editorial it looked at the current state of Digital Forensics where standards are concerned (Marshall 2011).

Google scholar was also used in the search for related information. The results included a number of peer reviewed papers from various journals and conferences, articles, blog postings and guidelines written by organizations for their own use however no relevant peer reviewed research was found directly related to the topic of standards. Throughout all these searches a myriad of peer reviewed papers on digital forensics methodologies, methods and frameworks were found with the three terms being used interchangeably. It was found that while there were several methodologies in place there were no set standards available to guide/govern the digital forensics process. This leads to inconsistencies in the field and speculations with regards to the standard at which they should operate.

This section will describe existing digital forensics process models developed for investigation of digital incidents in private organizations as well as law enforcement. These methodologies/models/frameworks are developed by various organizations for internal investigations and/or training as well as academic purposes.

There are a myriad of existing digital forensic models, methodologies and frameworks, some of which have been developed by organisations for their own use, or by law enforcement personnel for their own countries and even by other individuals based on their background, personal objective or the needs of their employer's (Salemat et al 2008) and (Perumal 2009). These designs are also at times driven by the tools available to the investigator, the ones with which they may be familiar or the most economical. Additionally these designs focus on particular aspects of the digital forensics process more-so either the technical or legal aspects of the investigation. There are some models that focus solely on the acquisition of the evidence ignoring all other processes that are critical to a "forensic" investigation. The models to be discussed are some of the more popular ones highlighted in the field by academics and practitioners and all have positive and negative attributes that will be highlighted in this section.

One of the earlier digital forensics investigation design to be developed was the Computer Forensics Process by (Pollit et al 1995). This model is comprised of four stages (i) acquisition, (ii) identification, (iii) evaluation, (iv) admission as evidence and stresses the point that the digital forensics process should conform to the law while remaining committed to scientific principles. This model was designed with the object of acquiring evidence from crimes committed in cyberspace and focuses on the acquisition and identification of data in a networked setting.

(Kruse and Heiser 2001) was also one of the earlier models to be developed, published approximately six years after Pollitt's. It has three basic steps depicting the entire digital forensics process. The focus of this model is on the core aspects of digital evidence acquisition, authentication and analyzing the evidence. There is no inclusion of preparation for the process, seeking authorization to acquire the evidence or identifying the evidence. This methodology does not cover the entire forensics investigative process.

In 2001 the United States National Institute of Justice developed a model to guide first responders in the field. This guide references the different types of electronic evidence and also includes procedures on how to handle digital evidence. The emphasis of this model is on the collection process being oriented towards practitioners who respond to a physical crime scene. This result in very little detail is given on other sections. The phases of this model include: (i) Preparation: where practitioners prepare the tools and other equipment that will be used throughout the investigation. (ii) Collection: at which point the searching for evidence, documentation of the evidence as well as the collecting and copying of the physical objects that contain digital evidence is done. (iii) Examination: at this point the practitioner documents the contents of the system as well as does data reduction to identify the relevant evidence. (iv) Analysis – during this process the evidence found in the previous phase is analyzed to determine its significance and value to the case. The (v) reporting sees the production of notes from the examination and analysis of the evidence.

This model while almost complete, it excludes particular important instruction and focuses on the collection of the evidence over the other phases which are all integral to the digital forensics process. The model does not include a reconstruction of the scene of the incident or the development of an intruder profile.

Other existing models include HC Lee's which was developed also in 2001 H. C. Lee in his book 'Henry Lee's Crime Scene handbook' suggested a procedure that included an additional stage to that of (Kruse and Heiser 2001). This model is more systematic and follows four very pertinent stages, which are (i) recognition, (ii) identification, (iii) individualization and (iv) reconstruction. This model as alluded to before is similar to the previous methodology proposed by Kruse and Heiser assuming/ignoring particular phases of the forensics process and does not make accommodations for procedures to preserve the acquired data or that of seeking authorization to access the evidence or device contacting the evidence. This model focuses mainly on the analysis of the evidence however it does include the reconstruction of the digital crime scene.

There is also a methodology developed at the Digital Forensic research workshop (DFRWS) for the Digital Forensic process. This model is more extensive than the previous models highlighted. It has seven stages and makes far fewer assumptions than the previous models covering integral stages not previously covered. However like a number of the other models, it ignores or assumes some of the legal aspects of the investigation and focuses more on the technical aspects. It includes the stage “decision” which is somewhat out of the remit of the forensics process, which is concerned mainly with investigation and presentation of the findings.

In 2002, Reith, Carr and Gunsch proposed a model that had a number of phases in which at least two phases overlap. This model is based on the one developed by DFRWS earlier (DRFWS, 2002). The phases proposed include (i) identify, (ii) prepare, (iii) approach strategy, (iv) preserve, (v) collect, (vi) examine, (vii) analyse, (viii) present and (ix) return evidence. This model, despite addressing some of the core areas of forensics, and is a good reflection of the digital forensics process, does not include any suggestion of getting authorisation to preserve and /or collect the evidence, which is very important with regards to the legal aspects of any forensics process. This may also present a risk to the overall accuracy of the investigation. Another drawback of this model as supported by (Tushambe 2004) is that the third phase of this methodology (The approach strategy) is a repeat of the second phase (preparation).

The integrated digital investigation process created by Carrier and Spafford in 2003 is based on the investigation of a physical crime scene. In this framework the digital crime scene is defined as a ‘virtual environment’ created by software and hardware where digital evidence of a crime exists (Carrier and Spafford 2003). The framework is organised into five groups with a total of seventeen (17) phases. It highlights the reconstruction of the events that led to the incident and promotes the reviewing of what was done throughout the process. This model gives real in-depth step by step description of the digital forensics process with somewhat of a focus on the investigation phase itself. The phases of this methodology are:
(i) Preservation, which sees the preservation of the preservation of the crime scene. Survey described as the search for the obvious evidence relevant to the case. Somewhat similar to that of e discovery, including elements of the e-discovery process. (ii) Document, the creating documentation of the crime scene. (iii) Search, during this phase the practitioner will conduct a more thorough search for any evidence not found in the survey phase. (iv) Event Reconstruction, at this point the practitioner reconstructs what happened from the digital events that occurred at the crime scene. This model superficially covers some of the integral parts of the digital forensics process with no creation of creating an intruder profile.

(Eoghan Casey 2004) proposed one of the more popular models as depicted in his book 'Digital Evidence and Computer Crime'. In this model Casey focuses on the investigation itself and presents only four stages that are (i) recognition, (ii) preservation, (iii) classification and (iv) reconstruction. Similar to some of the previous models Casey's model focuses on the examination on the model itself and is a highly technical model. It however depicts relationships between the legal technical and general forensics science concepts. While the legal facet is accounted for there is not much emphasis placed on the legal adherence of the presentation of the findings which is an integral part of the digital forensics process.

One of the most comprehensive models developed for the digital forensics process is the model created by Ciarhuain to address cybercrime in Malaysia that was published in 2004. This model depicts definitive steps to be taken by a digital forensics practitioner. Considered by other researchers such as (Salemat et al 2008) to be "one of the most complete digital forensics models up to then", it provides a basis for the development of tools and techniques to support the work of the digital forensics practitioners. The model starts out with a preparation for the investigation phase and goes through thirteen phases/activities to the dissemination of the information. This model, unlike the others, does specify phases pertinent to a digital forensics investigation but has been developed to address cyber related crimes (cyber forensics) and developed specifically for the Malaysian context. A number of the stages are also redundant and the need for preservation of the acquired evidence is not mentioned which is integral in ensuring the admissibility of the evidence should it be required for use in court.

The model by Bogen and Dampier was developed in 2005 and has three distinct phases and is referred to as a multi-view computer forensics model. The views are investigative process view, domain view and evidence view. Each view has related products including models and dependencies. This approach is quite different from the others identified and does not directly build or expand on a preceding model. It was designed from a software engineering standpoint and is thus focussed on the technical aspects of the digital forensics process.

Having concluded that the models/frameworks/methodologies preceding 2005 were single tiered Beebe and Clarke developed a models that to reflect the perceived multi-tiered process of digital forensics. They suggest that this framework offered practical and specific benefits not offered by such work as that of (Carrier and Spafford 2003) (Salemat et al 2008). This framework is delineated by two phases and proposes several sub tasks for its digital analysis phase presenting a survey, extract and examine approach forming the second tier of the framework. The first tier of framework phases include, (i) incident response, (ii) data collection and (iii) analysis, (iv) presentation and (v) closure.

First Tier:

Preparation: preparing the resources needed for the investigation.

Incident Response: Going in and assessing the incident to determine an appropriate approach

Data Collection: Gathering the digital evidence to support the approach strategy

Data Analysis {Further organized into the second tier}

Presentation: Communicating the findings of the investigation to the stakeholders

Incident closure: Reflecting on the process and make adjustments if needed.

Second Tier:

Survey:

Extract: During this phase the data is extracted based on the objectives of the investigation. This will involve the use of techniques such as filtering and keyword match searching.

Examine: The extracted data is examined. The objectives of the investigation are then confirmed or refuted.

Whereas this model covers all the phases and activities in the previous models such as that of (Reith et al 2002) it focus is mainly on the investigative phase of the digital forensics process. The model does not cater to the legal issues associated with investigating a computer related criminal activity, creation of an intruder profile or reconstruction of the crime scene.

Carlton in 2007 developed comprehensive work as a result of analysis performed on data collected from digital forensics practitioners of technical and legal backgrounds. It identifies 103 tasks performed by digital forensics practitioners as it relates to digital data acquisition. The development does not cover the reporting phase, it however does make mention of getting legal authorization to seize and search as well as maintaining a chain of custody. This model as alluded to before focuses on the Investigative (specifically the data acquisition) phase of the digital forensics process it however excludes presentation, intruder profiling and reconstruction of crime scene.

Another model to be mentioned was developed by Yong-Dal, in 2008, has network forensics at its core and is not openly general, though it could possibly be adapted. Yong Dal’s model focuses on the investigation of crimes committed in cyberspace and includes phases such as

(i) preparation, (ii) classification of the cybercrime, (iii) deciding investigation priority among others. It takes the investigator through summoning the suspect (which is not a core responsibility of a forensic expert) to writing the report. A comprehensive set of steps presented for investigation cyber crime however very little explanation is provided and including of steps out of the remit of the digital forensics practitioner.

Two of the more recent models (Salemat et al 2008) and (Perumal 2009) are the more comprehensive of the existing models. In an article entitled "The Mapping process of Digital forensics Investigations" (Salemat et al 2008), Salemat et al noted, "No formal theory exists for the digital examinations process". This is a point supported by (Perumal 2009), (Ricci 2006), among others. Salemat et al then proceed to produce what they term the "mapping process of the digital forensics investigations framework". The output of this process is a combination of the previous frameworks eliminating redundancies and detailed explanations of particular steps that were deemed vague. This has resulted in a five-phase step of activities with the headings, (i) preparation, (ii) collection and preservation, (iii) examination and analysis, (iv) presentation and (v) reporting. This structure of activities is written specifically for the Malaysian Criminal Justice system. It is very comprehensive and addresses key areas such authorization (but not continuous legal adherence or ethics), live and static data acquisition for use as evidence (not filtering of pertinent/relevant evidence) and storage of data. Overall Salemat's model is a very comprehensive methodology; however the focus of the model is on data acquisition and does not include the presentation aspect which is a critical part of any forensics process as one of the objectives of forensics is to present the findings of the investigation.

The US Department of justice also developed a forensics process model. This model has four distinct phases:

(i). The Collection phase that includes evidence search, recognition, collection and documentation.

(ii). The Examination phase involves attempting to reveal hidden data establishing its relevance and origin.

(iii). The Analysis involves establishing the value of the evidence to case.

(iv). The Reporting phase which as with other models entail the production of a written report outlining the process taken to acquire the evidence relevant to the investigation.

This model does not accommodate the legal intricacies of the digital forensic process. It begins at the collection phase and does not cater for the important fact of receiving authorisation to collect evidence.

The APCO guidelines were developed in the United Kingdom to guide practitioners dealing with electronic evidence. The guide starts at scene with incident response techniques or assessment of the case mentioned. The document focuses on the recovery of the evidence and written mainly for law enforcement but may be adopted for private organisation. The focus of these guidelines is on the preservation and integrity of the digital evidence produced form the digital forensics process. The guidelines do not take into consideration all the laws that may impact on the process and is based on four main principles:

- (i) No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
- (ii) In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and implications of their actions.
- (iii) An audit trail or other record of all processes applied to the computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- (iv) The person in charge of the investigation (case officer) has overall responsibility for ensuring that the laws and these principles are adhered to.

These guidelines are generally accepted in the United Kingdom they are however not compulsory and different groups and organisations may devise their own.

There are a number of published papers presenting different methodologies, frameworks and models for digital forensics some of which have been highlighted. These designs as alluded to in other sections of this work focus on different areas of digital forensics or do not cover the entire process. The myriad of existing digital forensics methodologies, methods and frameworks in the field include: The integrated digital investigation process model (Kohn 2012), FORZA (Leong 2006), CTOSE (*Cyber Tools On-Line Search for Evidence),* (Khon et al 2008)and (Hewling 2011) however they too do not satisfy the requirements as ascertained from the survey paper developed by the researcher and posses similar loop holes to those identified in other models presented in this review. The importance of digital evidence in a technologically driven society cannot be overstated and thus there is need for consistency in the process used to acquire this evidence.

Model/Designer	**Year**	**Strengths (Includes)**	**Weaknesses (Excludes)**
M. Pollitt	1995	Identification	Authorisation Live acquisition
W Kruse II., G Hieser	2001	Authentication	Authorisation Live acquisition
H. Lee	2001	Identification Reconstruction	Preservation Authorisation Presentation Moving of evidence to controlled area.
M. Reith, C. Carr, G. Gunsh	2002	Identification	Authorisation Live acquisition Moving of evidence to controlled area.
Carrier and Spafford	2003	Physical crime scene setting Reconstruction of crime scene	Moving of evidence to controlled area.
E. Casey	2004	Identification Reconstruction	Focus is on the investigation Authorisation Moving of evidence to controlled area.
S. O. Cuardhuian	2004	Awareness	Preservation Cybercrime Focus Overlapping of steps Live acquisition
C. Bogen & D. Dampier	2005	Includes various digital devices	Technical Oriented
FORZA – R. Ieong	2006	Legal inclusion	Focuses on legal aspects
Carlton	2007	Focuses on technical Specifically (data acquisition)	No Reporting, chain of custody, intruder profiling or reconstruction of crime scene.
ACPO	2007	Covers the recovery process.	Focuses on the collection of the evidence. Does not address specific laws.
Y.D. Shin	2008	Criminal profiling Classification of crime	Legal aspects
Us Department of Justice	2008	Does not differentiate between devices. Includes crime scene control and traditional forensics methods.	Focuses on first responders Very little guidance to investigating the actual system
S. Perumal	2009	Archiving	Classification of crime

Table 2.1 showing comparisons of some of the existing digital forensics models.

The revision of the aforementioned methodologies, models and frameworks highlighted a number of issues.

The major concerns arising from examination of the procedures identified include:

a. Lack of legal authorisation to acquire and examine the evidence. Legal authorisation to conduct the digital forensic process is integral to any investigation. Whether the investigation is being carried out by Law enforcement in a matter directly related to criminal activity or a private investigator doing a routine check for a private organisation.

b. The need for preservation of all evidence immediately. The majority of the methodologies reviewed assumed preservation of the crime scene and did not point to it specifically throughout the process.

c. The identification of the fact that a controlled environment is needed to carry out most of the investigation. The nature of digital evidence makes it vulnerable to accidental and deliberate changes. Operating in a controlled environment helps to mitigate the possibilities of data corruption and spoliation of evidence.

d. A step-by-step directive that can be followed by practitioners (usually provided with the tools but not good enough as the instructions are dependent on the developer of the tool).

e. The methodologies do not having any particular tools identified to be used at the different stages. The methodology was written in isolation, separate from the tools. (NB Carrier has addressed this concern somewhat with sleuth kit). There are a myriad of opens source as well as commercial available tools for digital forensics. Different tools are available for aspects of the process mainly acquisition, examination and analysis. A complete digital forensics methodology would adequately address this issue.

f. Reconstruction of the incident scene to enable accurate criminal profiling is not addressed by many of these methodologies. The main objective of a digital forensics investigation is ascertaining who did what when, where and how. Reconstructing the incident scene helps the investigator adequately retrace what happened leading to more accurate findings making it more likely to identify the perpetrator.

g. Both live and static data needs to be captured in digital forensics. Digital investigations will require acquisition of live and/or static data and thus any methodology developed should be done so to accommodate both.

The research has been designed to eliminate these issues. The 2IR methodology emphasizes the need for legal authorization from the onset. The designed application incorporates this by not allowing the practitioner to continue unless there is confirmation of the receipt of legal authorization. The 2IR methodology presented is guided by a framework of standards that guide not only the forensic process but provides guidelines for the development of the field as a whole. This research also include a reconstruction of the crime scene and the creation of an intruder profile as part of the methodology, both of which could prove invaluable to making conclusions in any digital forensic investigation.

Additionally, the methodologies, models or frameworks reviewed did not include much accommodation for education and training. As it relates to the definition of frameworks there is no existing framework of standards for digital forensics however there is a large number of existing digital forensics methodologies and models. An extensive review of literature revealed that much of the materials developed for digital forensics is not necessarily supported by empirical data but developed by commercial companies that produce tools for the digital forensics process. This point is confirmed by (Carlton 2007) where he notes "… much of the protocols, instructional materials and training courses available for computer forensics were largely based on anecdotal opinions or experiences of authors and instructors". This situation leaves the field open to being ad hoc with a lack of uniformity in how the field develops. An extensive review of the models preceding 2011 reveal that only two were found to be supported by empirical data, (Carrier 2006) and (Carlton 2006). The 2IR designed and presented in this research are supported by empirical data. They were developed as a result of identifying a need in the field and then further tested for appropriateness and practical use.

2.4 Digital Forensics Tools

Judges, juries and other officers of the courts rely extensively on the testimonies of expert witnesses to ensure the understanding of the technology involved in digital forensics. These expert witnesses in this case are mostly digital forensics practitioners who in turn rely on developed digital forensics tools in the process of acquiring and interpreting digital evidence. While there are some practitioners who develop their own tools for use [see case 10: Casey Anthony Section 2.2.3] there is a large commercial market for digital forensics tools as well as a myriad of open source options. The field being driven by commercial interest leaves it open to be manipulated for financial gain as opposed to the focus being placed on the development of the field. Being directed by open source tools on the other hand shifts the focus to a more technically oriented field as opposed to there being a balance of all the facets in the field.

Digital forensics tools are the actual drivers of the digital forensics industry as without them a cybercrime or computer crime investigation cannot be carried out. The tools have for the most part been reliable and produce results that have been used in courts. This, despite there being no evidence of the practitioner using them being provided with in-depth information on how the tool actually works or the methods they employ enabling them (practitioner) to be able to verify the authenticity of the evidence received. Carrier (2004) notes with regards to digital forensics tools, "…They provide the investigator with access to the evidence but typically do not provide access to methods for verifying that the evidence is reliable". This situation could lead to issues if the practitioner is inexperienced. Digital forensics practitioners in the field need to be aware of how the tools they use work as well as verification methods to ensure that the resulting evidence is reliable and relevant.

Digital forensics tools are classified based on their role in the digital forensics process, the specific device they are developed for or a specific operating system. The roles include evidence acquisition tools, tools for examining the evidence, evidence analysis tools and integrated tools. The following is a description of the different groups of tools giving examples.

- Acquisition tools

Digital forensics acquisition tools are the set of tools that are used to make what is referred to as a mirror copy or image of the suspect device. This cryptographic hash is usually made at the time of acquisition and is one of the integral actions involved in maintaining the chain of custody of the evidence. This part of the digital investigation process is very important and the ultimate objective here is to preserve the integrity of the suspect device. It also in turn helps in maintaining the integrity of the evidence as it preserves the physical evidence from which the digital evidence will be acquired thus maintaining the chain of custody. Digital forensics acquisition tools are usually used in collaboration with write blockers to ensure that nothing is written to the drive during the process. Despite all good intents and purpose one needs to consider that there will be questions arising re the integrity of the copy being made. How does one prove that the copy is a complete copy of the original and how does one know for a fact that the copy and the original are the same? The answer lies for the most part in the integrity of tools being used as well as the integrity of the practitioner. These issues are addressed in the work being presented by this research as it includes the discussion of ethical principles and the presentation of a complete section for ethics on the framework.

- Examination and Analysis Tools

The tools used for examination and analysis are at times rolled into one. These tools are used to extract and analyze the digital evidence. Extraction may be of two types, physical and/ or logical. Physical extraction being the recovery of data all across the entire drive regardless of the type of file system while logical extraction recovers files based on the devices operating and file systems as well as its application (NCJRS nd).

- Multipurpose (integrated) tools

These are tools are those with different roles entwined into one tool. |These tools are able to carry out search, data acquisition, navigation extraction, examination and analysis along with reporting or two or more of those processes. These tools are usually the ones developed for specific devices or interfaces. Two examples of integrated tools are Encase (Guidance Software) and FTK (Access Data).

The data acquisition aspect of these tools facilitates the copying of or the making of a mirror image of the system of the device to be investigated.

The search aspects of these tools facilitates the identification of data that match a particular criteria (ranges, classifications) as stipulated by the practitioner.

The navigations aspects of the tools that carry such a feature facilitates the exploring of a digital crime scene enabling the practitioner to visualize the scene (Schatz 2007)

The extraction feature of a digital forensics tool facilitates the extraction of data such as internet browser artifacts.

Examination and analysis tools facilitate the practitioner in gathering valuable relevant information from the data gathered.

Integrated tools (Case Management tools) have emerged as a solution to the growing problem of increasing volumes of data sets that contain potential evidence (Schatz 2007) providing various ways of searching, filtering and analyzing the data found. Integrated tools also address the need for having a tool that provides all the services rolled into one as opposed to the acquisition of different tools for each function helping to alleviate some cost. These tools including FTK and Encase uses various techniques to assist the practitioner throughout the digital forensic process producing verifiable digital evidence.

There are a number of digital forensics tools available, developed by various different organizations and groups with different objectives. Despite the fact that these tools drive the technical development of the digital forensics field they also demonstrate or reinforce the ad hoc manner with which the field operates. There are a number of these tools available online free of charge and are often the tools used in training this leaves the field open to number of disparities. This research aims to address a number of issues existing in the digital forensics field including that of the tools used throughout the training of practitioners. Section 2.5 discusses some existing issues in the field with regards to education.

At present the field is driven by merchants who produce the tools used in the digital forensics process without much collaboration much between academic, legal and other stakeholders(Pollit and Noblet 2000) and (Carlton 2007). The approach to the digital forensics process is currently portrayed as being disjointed and ad hoc. There are a myriad of tools available to assist with a digital forensics investigation while the producers of these tools are the lead trainers for the sector suggesting that the field is tool driven, and biased in a technological/technical direction. (Nance et al, 2010)(Tu et al, 2013). The results for these tools used in an investigation may be accurate (being the tool that the examiner is trained to use), however the analysis and interpretation of the results may not be so. There is also the issue of the practitioner not being able to identify if a tool does not perform as it is required to. Such a situation will, and continues to, give rise to many questions when digital forensics is presented in a legal setting.

The fundamentals of any digitally related criminal activity lies in "digital evidence". This evidence is acquired through the digital forensic process, which is an investigative process involving the collection, preservation, interpretation and presentation of evidence. This process as described may differ from one investigator to another despite the various legislations in place. A fact highlighted in the survey where respondents were asked to give their definition of Digital forensics. Digital evidence is unique in a number of ways based mainly on the form it takes which is not necessarily a physical one. (Mercer 2004) points out "if someone opened a digital storage device they would see no letters, numbers or pictures on it". The very nature of the data highlights the need for a digital forensic investigator to be thorough in carrying out their duties.

The term *Digital Evidence* is defined by (Casey 2011) as, "Encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator”. The same term may also be defined to be, any data or information found to have been stored or transmitted in a digital form that may be used in court, (Hewling 2010). This type of evidence has become increasingly popular in recent years, as courts have begun to accept electronic based evidence for use in traditional cases.

As with any other type of evidence due diligence must be followed to ensure its reliability in a court of law and most courts have found it necessary to question the reliability of such evidence when presented. (United States v Carey and United States v Benedict).

This concern has been highlighted in several scenarios with the lack of standardization in the acquisition of digital evidence (i.e. Computer forensic methodologies) being blamed. (Casey 2004) supports this point stating, “Digital investigators do not have a systematic method for stating the certainty they are placing the digital evidence that they are using to reach their conclusions”. The methodologies and tools used by digital forensic investigators worldwide have been variable and there is no one internationally accepted benchmark. (Casey 2004) continues, “This lack of formalization makes it more difficult for courts and other decision makers to assess the reliability of digital evidence and the strength of the digital investigators’ conclusions”. This dilemma is further supported by (Fulbright and Jowoski 2006) where they state, “The number one problem in current litigation is the preservation and production of digital evidence”. The latter are two of the processes involved in the digital forensic process. The work presented in this project highlights how digital forensics investigative process can be standardized. By involving practitioners from different jurisdictions in its development and enabling contribution, from not only practitioners of different backgrounds, but also with different experiences from varying jurisdiction helping to place this methodology in the unique position of being used as an international benchmark for the field of digital forensics.

The problem of standardization in the area of digital forensics has been an issue from the initial stages and still faces major challenges when digital evidence is being presented in court. (See case Coleman Holdings Inc v Morgan Stanley). “Because computer forensics is a new discipline, there is little standardization and consistency across courts and industry” [USCERT]. It is integral that agencies and practitioners adhere to a defined set of standards and operating procedures to ensure this evidence and methodology is accepted by the legal community. Bryan Sartin, (Managing director of Cybertrust) in an interview with SCmagazine states that there is still much more to be done where digital evidence acquired through computer forensic is concerned. He noted that, “There are two things missing: a single commonly accepted standard and uniform code of working…. Quality of service across computer forensic providers varies dramatically …” (Chaikin 2007) sums up the need for standardization within the sector when he argues; “…there is an absence of generally recognized standards of best practice in digital evidence forensic procedures, and a lack of adequate training of forensic examiners”. He makes a very valuable point when he continues his argument, “errors in analysis and interpretation of digital evidence are more likely where there is no standard procedure for collecting, preserving and analyzing digital evidence”. Such statements from seasoned practitioners in the field highlight the need for standardization of the procedures used in the digital forensics field.

The need for standardization in the field has been duly noted and this need cannot be emphasized too much.

2.5 Digital Forensics Education

While other forensic fields have a defined educational structure, digital forensics has not achieved maturity, and hence there is a clear absence of such a framework. Despite being in its development stages there are a number of other associated factors including the challenge that practitioners working in the digital forensics field come from a wide and diverse set of backgrounds, and that the field itself is driven by tool development, rather than a wider multi-disciplinary focus. These two factors present an enormous challenge to the emergence of digital forensics as an academic discipline. Digital Forensics, unlike other forensic disciplines, does not have an international body that sets rules and guidelines to ensure consistency in the field nor is there a set of standards to be used as a benchmark by practitioners worldwide (Nance et al 2010) and (Craiger et al 2007) ensuring that a particular standard of performance is maintained by all practitioners.

A major factor in enabling the acceptance of Digital Forensics as a discipline is having a structured approach to educating practitioners in the field. (Yanisec et al 2003) states; “a key step to improving forensics techniques lies in creating a comprehensive approach to forensics education”. The educational aspect of a field undoubtedly lies in research and education. As the demand for practitioners increase so does the demand for training and education in the field at all levels. A study by the Institute for Security Technology Studies at Darmouth

College found that 7% of computer crime investigators had no formal training, and only 11% had completed a full course of academic study in a related field while 90% of the respondents indicated that there is an urgent need for training and education. The need for proper education and training specific to the field of digital forensics is critical. Not only is it necessary to ensure the field is able to develop as a true forensics discipline but to ensure that the resulting digital evidence is relevant, valid and robust enough to withstand the rigors of a courtroom when being presented. See issues with digital evidence in cases presented in section 2.2. (Craiger et al. 2007). The forensic sciences however do not only require practitioners to have appropriate training and education, but also to be able to communicate the results clearly to a court which may contain a lay jury (Yansic et al 2003). For some, Digital forensics is a purely technical field and there is the need to refocus this thought and ensure that education and training in the field encompasses all facets. (Craiger et al 2007) states, “There is a common misconception among laypersons that digital forensics is primarily a technical field, dealing with computers and networks”. To this end academics, in designing training courses at all levels, must ensure that all facets of the field are compensated for. (Craiger et al. 2007) continues, although digital forensics does require a good deal of technical skills, it is just as important that students understand the legal basis for their actions”. The importance of designing a curriculum that integrates all aspects of Digital forensics cannot be over emphasized.

Education is an important factor in carving the way forward for digital forensics becoming a true forensics discipline. One of the critical factors is the widespread growth of cyber crimes which has prompted increased concerns. Some of the challenges cited in the fighting of technology related criminal activities included along with lack of standards, is the lack of education and training standards and adequate capabilities within law enforcement (Wolf 2009). (Kessler et al 2008) notes that the computer forensics community is concerned with the lack of education and training standards for digital forensics, a point which is supported by (Rogers and Siegfried 2004). With the continued impact of technologically related crimes on our society a number of educational institutions have begun to develop digital forensics programmes. Factors such as the privacy of information, the use of widely accessed personal information, legal issues associated with cyber crime activities and technology in general along with the opening up of once closed international borders has piqued the interest of a diverse range of people, thus resulting in the need for the training of a new set of professional to address the issues. Research undertaken by (Hewling 2010) revealed that there are a number of courses being offered worldwide by different institutions addressing digital forensics and the digital evidence acquired through the process. These courses are known by different names including cyber forensics, computer forensics, cyber investigations, digital investigations, digital forensics or based upon the specific area which they address such as incident response. A number of certification courses were found to be offered by different private organizations some based on a tool developed for digital forensics. This lack of consistency in how the training of digital forensics professionals is undertaken can present a number of issues regarding the digital evidence acquired specifically when it is to be presented in court. This, in turn, presents issues with the development of the field as a whole with various institutions and organizations doing their own training. The work on education presented in this research aims to address this issue by presenting an outline of courses that are to be included in a digital forensics curriculum. The research project as a whole highlights the need for coherence and standardization of the field including the training of digital forensics practitioners to ensure the reliability of the digital evidence uncovered in a digital forensics investigation.

In the United States there are several Universities offering digital/computer/cyber forensics either as a full degree course or as a module in a course. In the Caribbean there is one University that offers digital forensics as a part of a general information security course. In the United Kingdom there are several universities also that offer full degrees in the field as well as a part of a course such as information security. There is however still no standard educational guideline with regards to digital forensics science. In the United States there are general guidelines provided by the National Institute of Standards and Technology for digital forensics which include specific topics outlined for the development of Digital forensics curriculum. However as noted by (Tu et al. 2013) none of the existing educational training programmes have been implemented it as it is would prove too expensive for educational institutions to implement. There is thus need for the development of a curriculum that can be implemented by academic institutions without the added burden of exceptional cost. Such a curriculum would be a comprehensively developed education programme that integrates all aspects of digital forensics covering all disciplines involved, and will help to address the core problems facing the community such as reliability and consistency of the digital evidence produced.

Digital forensics, like other forensics sciences, requires practitioners to be appropriately trained in all key aspects of the field. They must not only be able to deliver scientifically valid results but must also be able to deliver these results orally to people from varying backgrounds. Such a programme would be a curriculum carefully designed for different levels of education as well as different categories of learners. Levels include; Certificate/Associate, undergraduate degree and postgraduate degree programmes. Categories of learners would include non-technical and technically oriented. Digital forensics is a multidisciplinary field that has its base in law and technology (computer, mobile devices etc.) taking in other fields associated with both such as laws of evidence, investigative techniques, operating systems among others. (Tu et al 2013) indicates that due to its multidisciplinary nature, digital forensics has to do with investigations, seizures and arrest as well as the preservations and storage of digital devices. They continue stating that "as such digital forensics education is composed of a large set of topics a point reinforced by (Yanisec 2001). As with the designing of any curriculum careful attention must be taken to include appropriate teaching methodologies, suitable teaching materials and a suitable, accessible learning environment appropriate to the facets of the field. The ideal would be a variety in each area. A thorough digital forensics programme should provide participants with particular core skills. These include practical experience in solving cases which could be in the form of case studies or working alongside practitioners, and understanding of the legal and ethical issues and the implications that they may have on an investigation, basic detailed technical computer-based skills and forensic based skills including collection, analysis of data and the reporting of findings.

At present the field is driven by merchants who produce the tools used in the digital forensics process without much collaboration much between academic, legal and other stakeholders(Pollit and Noblet 2000) and (Carlton 2007). The approach to the digital forensics process is currently portrayed as being disjointed and ad hoc. There are a myriad of tools available to assist with a digital forensics investigation while the producers of these tools are the lead trainers for the sector suggesting that the field is tool driven, and biased in a technological/technical direction. (Nance et al, 2010)(Tu et al, 2013). The results for these tools used in an investigation may be accurate (being the tool that the examiner is trained to use), however the analysis and interpretation of the results may not be so. There is also the issue of the practitioner not being able to identify if a tool does not perform as it is required to.

2.6 Summary

This chapter presented a discussion on the literature surrounding the various facets of digital forensics as well as an insight into how the presented work will address the significant issues and challenges identified to be existing within the digital forensics field.

Many practitioners in the digital forensics field have recognized that digital evidence is proving to be an integral part of cases being presented in courts, despite the origin of the case. Casey (2011), Hewling (2011), have made such observations in published work. The growing popularity of this new phenomena is proving a challenge to courts and thus the practitioners in the field must be concise in their practice. An integrated framework of standards encompassing all facets of the field with a step by step methodology that is designed incorporating these facets assists practitioners to be more concise and observe all possibilities while conducting their practice. The work presented in this research was designed to address these issues.

Huebner et al (2007) indicates that the first criminally prosecuted computer crime case was in 1966. They continue noting that the first computer forensic training course was in 1989 while the first specialized software tool emerged in the 1980s. Despite this wealth of history there is still no consensus on the exact meaning of related terms including what digital forensics is, or what cyber crime is. There are still no standards developed, an accepted methodology or an adequately defined body of knowledge (Huebner et al 2007), (Marshall 2011). The designing of this research included material and practitioners from various jurisdictions and aims to fill the need for a set of standards in the field of digital forensics.

There are more than twenty published papers discussing, analyzing and presenting methodologies, frameworks, and models for the acquisition of digital evidence (Carlton 2006, Carrier 2006, Yong-Dal 2008,). These designs all focus on different aspects of the digital forensics process and do not cover all the required steps of a forensics investigation. The importance of digital evidence is increasing in a technologically driven society and thus there is need for consistency and standardization in the process used to acquire and present this evidence after responding to a computer/cyber related incident. Cybercrimes are constantly and increasingly occurring and thus the response to this type of criminal activity must be able to produce evidence that is robust to assure successful prosecution of the guilty or acquittal of the innocent. Cyber related crimes will only become more sophisticated and technology continues to evolve, the measures in place such as the investigative methods, software and hardware tools as well as the laws must keep abreast. The research work done in this project is aimed at addressing the key problems and challenges faced by the digital forensics field and to ensure that the discipline is robust and thorough so that an accused can be effectively prosecuted and convicted or acquitted of a cyber related offence.

CHAPTER THREE

RESEARCH METHODOLOGIES

This chapter presents a discussion of research methodologies and paradigms including those inherent to Information Technology used within this thesis. It will continue to discuss the particular research methodology/s employed throughout this thesis along with a presentation and discussion of the particular procedures that took place throughout. The chapter also discusses the initial literature data collected.

3.1 Research Approaches

There are a number of paradigms that underline research in information technology (Clarke 2005). A paradigm according to (Kuhn 1970) is "the underlying assumptions and intellectual structure upon which research and development in a field of enquiry is based". (Patton 1990) defines it as "a world view, a general perspective, a way of breaking down the complexities of the real world". Paradigms include positivism and interpretism, qualitative and quantitative, inductive and deductive as well as explorative and confirmative. According to (Filstead 1979) a paradigm may serve a number of purposes including:

1. It guides professionals as it indicates important issues challenging a discipline.
2. It develops models and theories that permit practitioners to solve these issues.
3. It establishes criteria for tools such as methodology, instruments and data collection that would enable solving these issues.
4. It provides the principles, procedures and methods to be considered when similar issues appear.

3.1.1Positivism versus Interpretism

There are a few metatheoretical differences between the research approaches of the positivist and the interpretivist. In terms of onthology, which deals with the fundamentals of being; positivism assumes that the researcher and reality are separate while interpretism assumes they are inseparable (Stahl 2008). With regards to epistemology that deals with knowledge or the theory of knowledge, positivism assumes that objective reality exist beyond the human mind. Interpretism on the other hand assumes knowledge of this is intentionally built through lived experiences or social construction of the world. As it relates to what is being studied or research object, positivism assumes that the objects researched have particular qualities that exists independent of the researcher as opposed to interpretism which assumes a research object is interpreted based on meanings structured by the researcher's lived experiences. In terms of research methods, the research designs for obtaining data about the objects of the study positivist use a number of methods including laboratory experiments, survey and field experiments as research methods. Positivist usually gather large amounts of data and employ statistical and content analysis to analyse data and detect any existing irregularities. Interpretivist on the other hand use case studies, ethnographic, phenomemographic and ethno methodological studies as their research methods along with hermeneutics and phenomenology to make sense of indirect meanings and look into hidden ones. Validity in research measurement referring to the extent to which the test measures what it claims to also receives opposing views from the positivist and interpretivist. Positivists are deemed to collect data that are true measures of reality and thus makes the data collected valid. The approach of the positivist employ various types of validity checks such as construct validity, statistical conclusion along with internal and external validity. The interpretivist however are more concerned with the knowledge being acquired from research being defensible and thus assumes that evidence should be produced to support any claims made. Interpretivists on the other hand think the process used, as well as the research context, should be used in deciding the acceptance of the knowledge claimed. Positivist also believe that a research is reliable if the outcomes are the same if and when done by others. Positivists attribute lack of reliability, reliability of research as defined by (Joppe 2000), " The extent to which results are consistent over time and an accurate representation of the total population under study is referred to as reliability to factors such as researcher bias, errors in measurement, and inconsistency of the procedures used". Interpretivist however suggests that the research is reliable as long as the researcher can demonstrate interpretive awareness.

These supposed meta theoretical differences between the approaches of the positivist and the interpretivist are deemed to be "spurious" according to (Weber 2004). Weber continues, asserting that the differences lie in the choice of methods. Researchers deemed to be positivists use research methods such as surveys, field studies and experiments. Those researchers on the other hand who are deemed to be interpretivist are more likely to use methods such as case studies and ethno methodological studies. The difference in choice of research methods may be due to factors including type of training provided to the researcher, recommendations and/or pressure from advisors and colleagues. (Weber 2004) concludes "that it is time the rhetoric of positivism versus interpretism to rest, as it serves no useful purpose but instead promotes prejudice in research evaluation". He continues "The researcher's goal is to improve knowledge of a certain phenomena while at the same time acknowledging that different research methods and data analysis techniques have their own unique strengths and weaknesses depending on existing knowledge about a phenomenon". Whereas the methods chosen may differ, the objective in the end is to provide information that is useful to the field.

3.1.2 Qualitative vs. Quantitative

There are generally two main categories of research methodologies, quantitative and qualitative. Qualitative research revolves around the use of qualitative data such as published documents, interviews, and observations. Originally developing in the natural sciences to study natural phenomena, (Cohen et al 2011) it is now being used in different fields and disciplines. The objective of qualitative research is to answer a question or set of questions. The findings of a qualitative research are not determined in advanced and usually it produces findings that are applicable beyond the remit of the research, (Cohen et al 2011).

The major characteristics of qualitative research include discovery, exploration and induction. The researcher is the primary instrument in data collecting and theory building. It involves qualitative analysis and induction. Techniques employed in qualitative research include, in depth interviews, grounded research and focus groups. Quantitative research alternatively includes confirmation of theory, explanation, a standardized data collection and statistical analysis. Quantitative research revolves around the use of data collection methods such as closed ended questionnaires and structured interviews. The findings of quantitative research are based on numbers and definitive responses from participants. This type of research is based directly on initial research plans and is more easily analyzed and interpreted.

The qualitative and quantitative methodologies are paradigms based on the positivism interpretism juxtapositions. The quantitative paradigm is largely based on positivism a position that advocates (as alluded to before in this chapter) the existence of a position independent of human perception. The researcher and the object being investigated are separate with none influencing the other. Quantitative research employs empirical research under the belief that all phenomena can be reduced to empirical indicators representing truth (Weber 2004). The usual techniques used in a quantitative research will include surveys with some predetermined responses, highly structured rules for collecting data and randomization. The sample size in a quantitative research is usually larger than that of the qualitative.

The qualitative paradigm is however based on interpretivism. This indicates that it makes allowance for the role of the human mind in shaping the outcome. The researcher and the research are interdependent and findings are mutually created based on the context. Qualitative research stresses processes and employs techniques including in-depth interviews, focus groups and observation.

A mixed approach using both quantitative as well as qualitative methods could be deemed time consuming but is likely to produce a rich set of data. A mixed approach occurs when the research employs use of techniques, approaches and concepts from both the qualitative and quantitative realm. This type of research will include the inquiry methods of induction as well as deductive reasoning. The main idea behind the mixed approach is the ability to understand the strengths and weaknesses of the approaches and build on it to produce a superior study designed to mono-methodological studies because they combine complementary strengths and non-overlapping weaknesses. (Johnson and Turner, 2003) One of the first applications of mixing research methodologies has been attributed to (Campbell and Fiske 1959), they used multiple methods in their study of psychological trait validity (Creswell, 2008). Following this many researchers came to recognize the value of integrating both qualitative and quantitative methods in their work recognizing the value combining both as opposed to relying solely on either approach.

The use of a multi method research approach on the methodological level is one solution to the positions being argued. (Sale et al 2002) argue that because the two paradigms do not study the same phenomena, qualitative and quantitative methods cannot be combined for cross validation or triangulation purposes. Researchers advocating for the combination of methods argue that the different methods have different strengths and thus a combination of both would produce more than what each method would in isolation. (Morgan 1998) suggest that the mixing could be carried out on the technical aspect (means of generating knowledge), which can be done without violating basic paradigmatic assumptions.

The different inherent characteristics and methodologies used in these two paradigms may be used to complement each other. (Morgan 1998) proposed a matrix approach for using qualitative and quantitative research on the data collection level, where the classification is based on two types of decisions: priority and sequence. Figure shown below:

	Priority Decision	
	Principle Method: **Quantitative**	**Principle Method:** **Qualitative**
Complementary Method: Preliminary **Sequence Decision**	1. **Qualitative preliminary** ***Purpose:*** Smaller qualitative study helps guide the data collection in a principally quantitative study. - Can generate hypotheses; develop content for questionnaires and interventions, etc ***Example:*** use of focus groups help develop culturally sensitive versions of technology acceptance questionnaire.	2. **Quantitative preliminary** ***Purpose:*** Smaller quantitative study helps guide the data collection in a principally qualitative study. - Can guide purposive sampling; establish preliminary results to pursue in dept, etc. ***Example:*** A survey of different managerial level of an IT intensive site for more extensive stratified data collection.
Complementary Method : **Follow Up**	**3. Qualitative Follow – up** ***Purpose:*** Smaller qualitative study helps evaluate and interpret results from a principally quantitative study - Can provide interpretation for poorly understood results; help explain outliers. ***Example:*** In-depth interviews help to explain why one organization generates higher level of employee technology satisfaction/adoption.	**4. Quantitative follow up** ***Purpose:*** Smaller quantitative study helps evaluate and interpret results from a principally qualitative study. - Can generalize results to different samples; test elements of emergent theories etc. ***Example:*** An industry survey of different levels of information technology department pursues earlier results from a case study.

Table 3.1 Matrix for the use of both qualitative and quantitative methods at the data collection stage. Adapted from Priority Sequence Matrix, (Morgan 1998)

Number one on the table above (Priority sequence Matrix) depicts a research design where a smaller preliminary qualitative study provides complementary assistance in developing a larger quantitative study. In this case, although the major method employed is quantitative a qualitative method is used at the beginning in an effort to improve the effectiveness of the study. An example of this is starting a survey project with a focus group which is a qualitative method to analyse the content of a questionnaire This uses the strengths of the qualitative method for exploratory work in ensuring the survey covers the required topics (Cohen et al 2011). (On in this particular research the information found in the literature is validated by practitioners in the field).Number two on the table (Table 3.1) uses a small scale preliminary quantitative method to help in guiding the decisions a researcher makes in a large qualitative project. An example would be a preliminary census of a field to guide the selection of sites and information, providing a contextual understanding and helping to focus the analysis of large amounts of data. Number three depicts a research design that uses qualitative methods to complement a quantitative research project. In this case the qualitative method serves as a follow up to the quantitative study and typically provides interpretive results for understanding the results from a quantitative project. In number four the research is designed using quantitative studies as a follow up on research projects that are mainly qualitative. The quantitative method in this case is used as a means to expand on the results from the qualitative study.

There have been different perspectives on how the qualitative and quantitative methods of research may complement each other. (Johnson et al 2007) suggests that at the research design stage, quantitative data can help qualitative components for example by identifying members of a representative sample and spotting outlying observations. The qualitative data can also help quantitative components with conceptual as well as instrumental development. In an example at the data collection stage, quantitative data can help in providing baseline information to help avoid bias, whereas qualitative data can help to facilitate the assessment of quantitative data and give a new perspective on the findings. For decades researchers have argued regarding the methods and advantages of using a mixed method approach to research, there have also been arguments over the definition of the term mixed methods being used interchangeably with multi methods, (Johnson et al 2007) defines mixed methods as “the type of research in which a researcher or team of researchers combines elements of qualitative and quantitative research approaches”. The authors continues stating that as a research type a mixed methods study would involve mixing within a single study while on a program level it would involve a mix of methods within a programme of research .

Mixed methods research approaches, combining qualitative and quantitative methods is one way of describing the combination of both methods. Authors such as (Creswell 2003) have proposed research designs that consider the purpose of mixing methods throughout the research design and implementation process. (Maxwell and Loomis 2003) however propose an approach to mixed methods that differs from the others. This involves the design of a study consisting of five separate components, (i) purpose, (ii) conceptual framework, (iii) research questions, (iv) methods and (v) validity strategies. They consider this design to be a systematic or interactive model and while all five components can influence other components of the design the research questions play a central role. In the interactive design model the research questions are presented not as the starting point but as the heart of the design because they are innately linked to the other components. Therefore the research questions must inform and be responsive to these other components of the design. The focus of the interactive design is on the relationship that exists between both the qualitative and quantitative approach across all the five components.

Table 3.2 below highlights some of the data collection techniques that are used in both the qualitative and the quantitative research approach generally some of which are used in this research. The table highlights the strengths and weaknesses of each technique.

Collection technique	**Description**	**Advantages**	**Disadvantages**
Observation	Methods by which researchers gather first hand data on programs, processes or behaviours being studied.	1. Provides direct information about behaviour of individuals and groups. 2. provides good opportunities for identifying unanticipated outcomes. 3. permits the evaluator to enter into and understand the situation/context 4. exists in natural, unstructured and flexible settings.	1. expensive and time consuming. 2. Needs well trained and highly qualified observers and in some cases content experts. 3. may affect the behaviour of the participants. 4. Selective perception of the observer may distort the data. 5. the investigator has very little control 6. The behaviours observed may be atypical
In-depth interviews	A dialogue between a skilled interviewer and an interviewee with the goal being to elicit detailed material that can be used in an analysis.	1. Usually yields a rich set of data with new and valuable insights. 2. It allows for face to face contact. 3. Allows for the ability to experience the affect as well as the cognitive aspects of responses. 4. Enable the interviewer to explain, clarify questions that may yield valuable responses.	1. Can be expensive and time consuming. 2. Requires highly trained and qualified interviewers. 3. Interviewee may distort information due to recall error, selective perceptions and desire to please interviewer. 4. Flexibility can result in inconsistency of interviews. 5. the volume of information may be too large to transcribe or reduce.
Focus Groups	Combines elements of both	1. Quick and fairly easy to set	1. Susceptible to

	interviews and participant observations.	up. 2. Allows for the observation of group dynamics, discussion and firsthand insights into behaviours, attitudes and language. Useful in gaining insight into a topic that may prove difficult using other collection methods.	researcher/facilitator bias. 2. Facilitates the discussion being dominated and possibly sidetracked by and individual or a few individuals. 3. Data analysis may be time consuming and needs to be planned in advance. 4. May not provide valid information at the individual level. 5. Information may not be representative of other groups.
Document Studies	Existing records often provide insights into a group or setting where the people cannot be observed using another method.	1. Usually available locally and is inexpensive. 2. Grounded in the setting and language where they occur. 3. Useful for determining value and interest, positions, political climate, attitudes, trends and sequences. 4. Provide s and opportunity for study of trend over time.	1. May be incomplete. 2. May be inaccurate and of questionable authenticity 3. Locating the appropriate documents may present some challenges. 4. Analysis may be time consuming. 5. Access may be difficult.

Table 3.2 A comparative analysis of collection techniques (Frechtling and Shape 1997)

Additionally there are structured interviews which are another data collection technique. Its emphasis is to obtain answers to carefully phrased questions. The interviewees are usually trained to deviate only minimally from the wording of the questions to ensure uniformity. Structured interviews may be face to face, over the telephone or with the use of electronic devices (computers, tablets etc.). Questionnaires are another technique which can be very efficient when the researcher knows exactly what is required and how to measure the variables of interest (Sekaran 2003). Sekaran continues, Questionnaires may be administered in person, sent through the mail or distributed electronically (Google drive, survey monkey etc). Each method will have its own advantages and disadvantages regarding cost, time, ease of distribution and response rate. The qualitative, quantitative and mixed method approach to research projects all have their advantages and disadvantages. The choice of approach is dependent on a number of factors and each should be carefully weighed before deciding on a fool proof method.

Inductive Versus Deductive

Research methodology is also concerned with the two broad methods of reasoning, inductive and deductive. (Lancaster 2005) identifies deductive reasoning as being narrow in nature and concerned with testing and/or confirming hypothesis. Defined as "a set of techniques for applying rigorously testable theories in the real world in order to assess their validity (Lancaster 2005). It is the process by which researchers arrive at a reasoned conclusion by logical generalization of a known fact (Sekaran 2003). The initial step in the deductive process is the generation of theories and hypothesis. This generation of ideas can be based on personal experiences or may be hypothesis and theories that stemmed from a previous literature search that brought together the idea of others. It may also be based on a desire to find the solution to an existing problem. Following the generation of theories there is then the operationalisation of the concepts in the theories and hypothesis such that these concepts can be measured through empirical observations. The next step in the process will be to identify and decide between alternative techniques and approaches to measure the operationalised concepts. This will also include the selection and design for research methodology to be used such as research instrument, data collection methods and the methods for analysis and interpretation of empirical observations and measurements. The deductive process ends with the falsification and discarding steps. Here the researcher decides the extent to which the chosen theories and hypothesis are falsified and the extent to which parts of these theories and hypothesis if any remain unfalsified (Lancaster 2005). The deduction process is one of drawing from logical analysis, inferences that are supposedly conclusive.

Inductive reasoning is the process of reasoning in which the premises of an argument is believed to support the conclusion but do not ensure it. In deductive reasoning researchers observe certain phenomena and on this basis arrive at conclusions; they logically establish a general proposition based on observed phenomena (Sekaran 2003). Compared to deductive reasoning, inductive reasoning is more open-ended. The process of inductive reasoning is the opposite of that of deductive reasoning as it moves from more specific observations to broader theories and generalizations. Using the inductive approach the researchers starts with specific observations and measures. The detection of patterns and regularities followed by the formulation of provisional theories to be explored and developed into general conclusions (Trochime and Donnelly 2005).

There have been arguments for the combination of both the inductive and deductive approach. Whereas the deductive approach supplies the shape of the argument, the induction approach establishes agreement about one or more stages in argument. (Huber et al 2005) notes:

> *"The two forms of reasoning are connected in the observation stage: the researchers may observe patterns in the data that lead them to develop new theories and hypothesis (induction). Hence, inductive and deductive reasoning are interrelated: inductive is used to prove that a casual relationship exists and to establish premises(facts) on which the deduction is built. Casual relationships are often established by induction or else exists within the premises of deduction".*

Employing both reasoning approaches can result in a richer set to deductions contributing to any research.

Exploratory versus Confirmatory

These two dichotomies are also types of research. Confirmatory being employed when the researcher is seeking to test or confirm a pre specified relationship while exploratory is utilized when a researcher is interested in defining possible relationships in the most general form. (Gerring 2001) states "most social science research fall between the exploratory and confirmatory ideal, and confirmation in the generally favored model of analysis. Nevertheless, both research models are not without limitations . Exploratory research can be thought of as being inductive in nature, with advantages such as flexibility in generating hypothesis, (Meyers et al 2005). The process of exploratory research makes theory falsification difficult thus results tend to be over-fitted with a greater chance of bias. Confirmatory research on the other hand relies on statistical inferences with confirmatory analysis providing precise information using well established theories and methods while the deductive approach relies on having hypothesis first and then tests to answer specific questions.

3.2 Grounded theory

Grounded theory is a research methodology involving the discovery of theory through the analysis of data mainly used in qualitative research. Grounded theory involves a systematic generation of theory from the data gathered and takes in both deductive as well as inductive thinking. Grounded theory has three basic areas according to (Pandit 1996), (i) the conceptualization of the data rather than the data itself, (ii) the analysis of the data that leads to developing theories and (iii) the relationships between a group of concepts and a category or categories. In order to get these elements together, works in grounded theory involve overlapping and iterative steps from gathering data to the development of theory (Dick 2005). Its basic idea being to read and discover relationships between variables. Activities instrumental in grounded theory activity include; data collection, note taking, coding (open, axial and selective), memoing and writing up.

3.2.1 Data Collection

Like most research techniques the initial step in grounded theory is data collection. This is done via the use of open ended questionnaires, review of relevant literature and/or interviews (Cohen et al 2007). Due to the fact that in grounded theory data collection and analysis of data occur simultaneously the method of collecting data should be flexible and is open to change throughout. The instruments employed by this research included the review of relevant literature, interviews as well as questionnaires using both open and closed ended questions.

3.2.2 Note taking

Upon collecting the data careful note must be taken of similarities or particular themes that may arise. During this phase the researcher notes clearly the responses of the participants and one should try not to steer the responses to fit their own perceptions (Charmaz 2006). Note taking was employed during the review of the relevant literature to record findings and during interviews.

3.2.3 Coding

The basis of Grounded theory is that whatever the researcher comes across (observes) throughout the process of the study is considered data, anything that contributes to the general concepts of the theory being researched. To evaluate this rich set of data supplied/received from various sources are coded. Grounded theory facilitates three main types of coding. They are open coding, sometimes referred to as initial or substantive coding. In this phase the researcher reviews the transcripts from surveys, interviews and notes then creates codes reflecting common themes (Creswell 2008) and begin to define concepts and initial categories for better understanding. Axial Coding is defined by (Charmaz 2006) as “a set of procedures whereby data are out back together in new ways after coding”. During this phase the research narrows also the focus of the project, examining the data for interrelated concepts. Selective coding is the final stage of the coding process. It involves centralizing the concepts, bringing the concepts and ideas that emerged explaining all interrelations observed (Creswell 2008). Coding was employed following the literature survey. This facilitates the determination of particular patterns including omissions identified leading directly into memoing.

3.2.4 Memoing

This is the next major phase of Grounded Theory. This is the process of writing memos that organize trends to define categories and relationships (Dick 2005). The researcher at this stage is able to generate developing theories. Memos are critical in refining and keeping track of ideas that develop during the process. These can then be compared generating the relationship between ideas and concepts.

3.2.5 Writing up

This is the stage where the researcher will put all the findings together to produce valid conclusions for publishing. (Miles and Huberman 1994) note that validity is critical as it relies on the credibility of the published results representing the views of the study group and whether or not the study could be applied to groups outside those studied. Grounded Theory however does not rely on traditional methods of validating results due to the fact that it is a concurrent process of gathering data and analysing it that is important (Elliott and Lozenbatt, 2005).

The use of a combination of methods, combining techniques of both a quantitative and qualitative nature, facilitates a deeper understanding of research than individual use (Creswell 2008). Such an approach shows appreciation for the distinct nature of both the qualitative and quantitative approach to research.

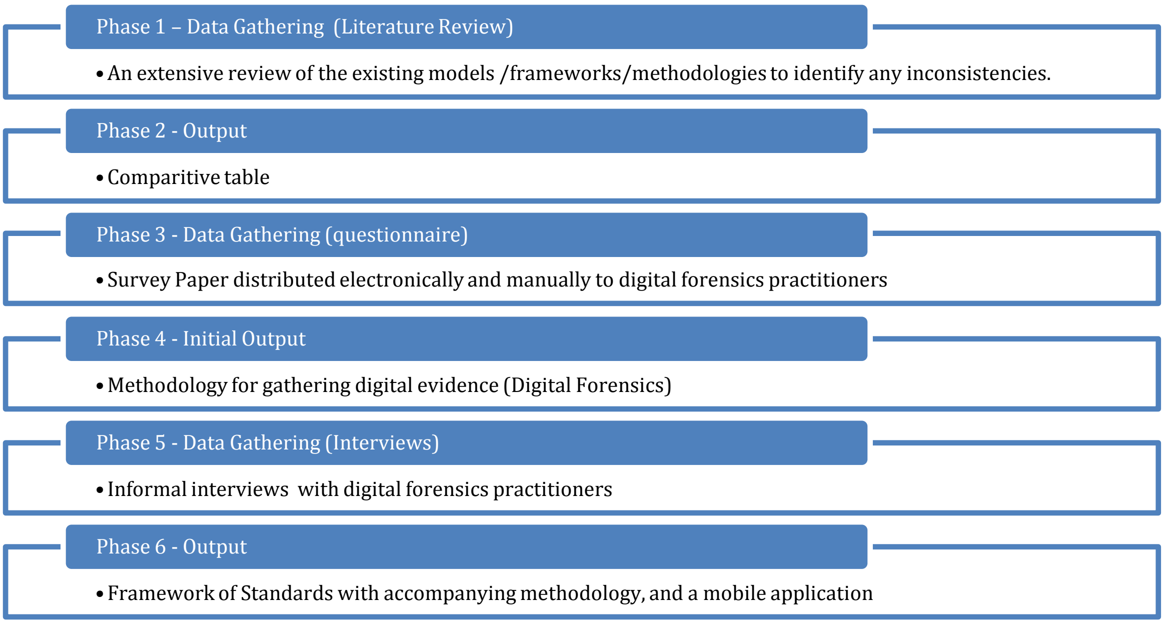
3.3 Approach adopted by this study

Researchers need to be motivated to acknowledge paradigmatic differences in methodology while attentively selecting the methods that provide the greatest opportunity for cross paradigm communication within the study design (Hall and Howard 2008). While some authors believe that researchers should adopt a model compatible with their research interest and at the same time remain open to other possibilities (Weber 2004) suggest that the different choice of research methods is mainly due to factors such as type of training provided for the research, social pressures associated with advisors and colleagues and preferences received from insight during research. Extensive research has been undertaken and different arguments have been presented for and against the different approaches to research which led to the choice of the approach taken in this study.

JUSTIFICATION OF APPROACH

The research plan outlined the need for the research to first collect and peruse academic papers published regarding digital forensics models/methodologies and frameworks. This review was expected to bring out certain patterns and information that would be further explored through a follow up survey. The research methodologies chosen for this study are based in part on studies conducted by (Carrier 2006), (Carlton 2007) and (Kessler 2010). These three practitioners have performed three of the largest digital forensics/digital evidence related studies to date. Like (Kessler 2010) and (Carlton 2007) this research project employs the grounded theory primarily because of lack of directly related empirical literature based on standards and guidelines in the digital forensics field. While there are a number of best practices and guidelines developed by different organizations and groups there is no evidence thus far of much empirical studies of standards and guidelines. The National Institute of Justice (United States Depart of Justice) in a special report entitles 'Forensics Examination of Digital Evidence: A Guide for Law Enforcement, carefully notes on the document "Opinions or points of view expressed in this document represent a consensus of the authors and do not represent the official position or policies of the US Department of Justice". It continues, "The products, manufacturers and organizations discussed in this document are presented for informational purposes only and do not constitute product approval or endorsement by the US Department of Justice". This research has a qualitative focus with some quantitative data to ensure a rich set of data while embracing the concepts of the grounded theory.

The stages of this study included three phases of data gathering with intermediate outputs before the final output.



Phase 1 – Data Gathering (Literature Review)

- An extensive review of the existing models /frameworks/methodologies to identify any inconsistencies.

Phase 2 - Output

- Comparitive table

Phase 3 - Data Gathering (questionnaire)

- Survey Paper distributed electronically and manually to digital forensics practitioners

Phase 4 - Initial Output

- Methodology for gathering digital evidence (Digital Forensics)

Phase 5 - Data Gathering (Interviews)

- Informal interviews with digital forensics practitioners

Phase 6 - Output

- Framework of Standards with accompanying methodology, and a mobile application

Figure 3.0-1 Processes undertaken by this research

Phase 1 Data Gathering {Literature}

The study began with the collection of academic papers written highlighting computer/digital forensics models/frameworks/methodologies and standards. This initial review included papers from a far back as (Pollitt 1995) up to (Casey 2011). The findings from the review of these papers were analyzed using Grounded Theory methods. These included note taking, coding and memoing.

Note taking - this involved the reading and analysing of academic literature and making notes of findings. These findings include what were the common concerns and exclusions. There was also note taking throughout the interviews as the researcher noted the responses of interviews, highlighting any concerns or suggestions.

Coding – This was employed throughout the life of the study but detailed mainly following the initial literature survey and interviews. Throughout the project the researcher sought to note any valuable information noticed from different sources that contributed the general concepts of the research. Sources included practitioners, academics, workshops, conferences, magazines, iTunes U presentations and Cousera open courses.

Memoing – It was in doing memos that the researcher identified developing trends and patterns from which the facets of the framework emerged. Memos helped the researcher to keep the ideas that emerged organized and together. Emerging ideas and concepts were then compared and developed.

Phase 2 Intermediate output

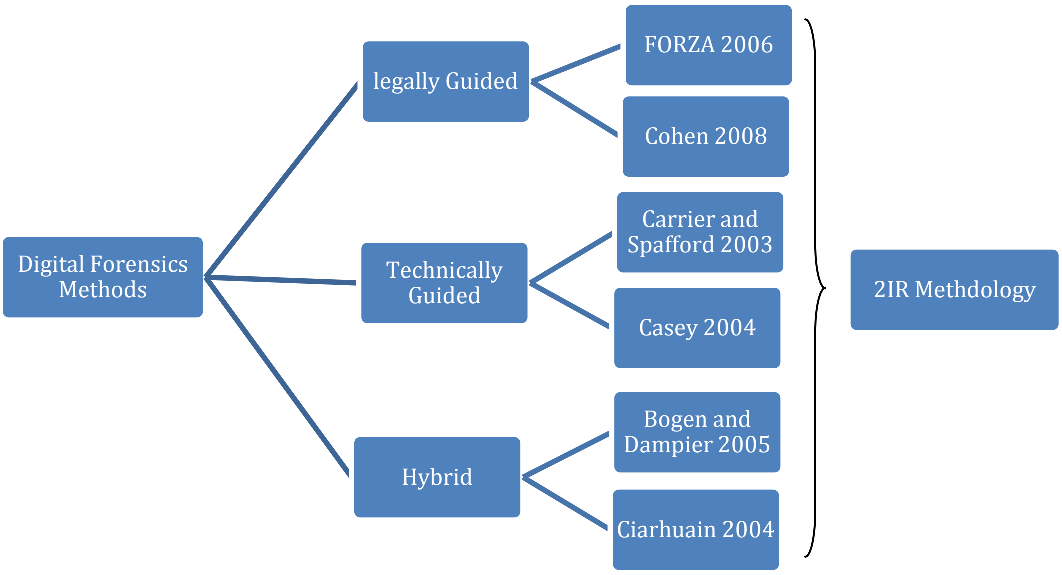


Figure 3.3 Classification of existing digital forensics models (from which the 2IR is designed)

Following phase one the review of literature related to digital forensics policies, methodologies, frameworks and methods, a table was produced (Chapter 2) listing the recurring themes. This table outlined ~~all the~~ digital forensics and digital evidence acquisition methodologies/models/frameworks since 1995. It is important to note that no standards were found. They were analyzed for their steps, inclusions, exclusions and note taken of the year they were developed.

Phase 3 Data Gathering – Initial survey paper

This phase began with a written survey paper with the objective being to gather information from practitioners re the digital forensics method/model/frameworks used if any in their practice. A total of eighty (80) practitioners' responses were used in this phase of data gathering. These results were then analyzed using the Grounded theory techniques (Quantitative) as well as some qualitative techniques with a questionnaire being designed using both open ended and closed ended questions. Responses were received from more than eighty (80) practitioners (ninety one (91) and filtering was done resulting in eighty (80) being used as further discussed in section 3.3.

Phase 4 – Initial Output

Following the analysis of the initial survey paper a framework (The 2IR framework) and companying methodology (The 2IR Methodology) to be used by practitioners in the digital forensics field was developed. These were designed based on the responses of the survey paper along with theoretical research findings highlighting shortcomings in the field. This was then distributed to a select group leading to the following phase.

Phase 5a – Data Gathering Interviews.

Interviews were conducted with practitioners from the USA, Europe, Caribbean and United Kingdom. These interviews were carried out as a follow up to the previous phase. Thirty one practitioners in the field from different professional backgrounds (technical, legal, law enforcement) were interviewed. The interview transcripts were analyzed using Grounded theory techniques to identify recurring themes. Detailed findings of this discussion is presented in chapter 5 section 2.

Phase 5b – Data gathering

A small survey of four questions was administered to the respondents during the interviews. This required comments on the need for more training in the field being researched. See appendix E for results and proposed curriculum designed.

Phase 6 Output

The output of this research project is the design of an overarching framework to guide practitioners in the digital forensics field. This framework of standards include guidelines from the four main facets of the digital forensics field; legal, technical, educational and ethical. The second deliverable is a step by step methodology indicating the phases and stages of the digital process. This methodology is accompanied by an application to further ensure that the standards as laid out in the framework are adhered to carrying out the process using the methodology. The output also includes a proposed curriculum for digital forensics practitioners addressing three levels of training; certificate, undergraduate and post graduate.

The research project employed a combination of research methodologies and paradigms throughout its duration. This to ensure that there was a rich set of data as a combination of methods are deemed to produce much more than one method can in isolation as they complement each other.

3.4 Initial Survey paper – Phase 3

In order to substantiate information gathered from various peer reviewed literature relating to digital forensics standards, frameworks and methodologies a questionnaire was designed seeking contributions from practitioners and other persons in the digital forensics field. This was done with an objective to validate assumptions with regards to the need for standardization in the acquisition and presentation of digital evidence from those who have practical experience of undertaking such investigations. The major aim of this survey was to ascertain the actual state of digital forensics examination and also for comparison to peer reviewed literature. The questionnaire targeted digital forensics practitioners with different backgrounds based on the field in which they work for example legal or law enforcement. The cohort included students, academics, law enforcement officers, lawyers and "forensicators", persons from a technical background peforming digital forensics investigations. The main question to be answered was: Is the digital forensics process as ad hoc in the real world as it has been theorized to be?

The initial survey paper had as its main purpose to find out if the findings of the literature reviewed correlated with what is happening in the field of practice.

Question1

The survey sought to ascertain the diversity of the background of digital forensics practitioners. This to establish the background skills of the persons currently employed as digital forensics practitioner. Question one thus asked practitioners to check their background from the list of choices given, legal, law enforcement, management, technical.

Question 2

The research sought to ascertain the relative level of experience that practitioners in the field, how long despite their background were they working as a digital forensics practitioner. Respondents were thus asked to indicate the number of years they had been practicing in the field. This also helps to quantify the literature that suggest that digital forensics has come to the fore since approximately 1995.

Question 3

The research sought to receive responses for a wide geographical area and thus practitioners were asked to indicate the jurisdiction in which they practiced. The choice presented were, Asia, Africa, Europe, Russia, North America, Caribbean, Middle East, Other.

Question 4

The research sought to ascertain the current working level that practitioners in the field, what type of work despite their background were they were doing as a digital forensics practitioner. Respondents were thus asked to indicate whether they were currently a student, practicing practitioner or other.

Question 5

To ascertain the consistency in the concept of what digital forensics is and its definition in the field, question six on the survey questionnaire asked that each respondent define the term digital forensics.

Question 6

In an effort ascertain the consistency in the concept of what digital forensics is and its definition in the field, question six on the survey questionnaire asked that each respondent define the term digital forensics.

Question 7

Literature review suggest that there has been an increase in cyber crime activity. The research sought to correlate this assertion with the request received for digital forensics services. This question therefore asked respondents to indicate how often they receive request for digital forensics services.

Question 8/9

In an effort to ascertain the current state of digital forensic procedures with regards to procedures used to carry out a digital forensic investigation and the existence or need thereof for standards in the field practitioners were asked to respond to the question; Are there policies in place to guide the digital forensics process? With the options Yes No This question was followed by another related question. Were these policies; with the options, developed in house, bought from a commercial organisation, adapted, other.

Question 10

In keeping with the theme of methodologies used the respondents were asked if they used any particular established methodology when conducting investigations regarding digital evidence.

Question 11

To get a detailed insight on how the process was carried out practitioners were asked to indicate the steps they too from the beginning of an investigation to the end. They were also asked in separate questions to indicate the initial step taken and the last step taken with regards to a digital forensics investigation.

Question 12

The researcher in an effort to rationalise the inconsistencies portrayed by literature in the field an attempt was made to ascertain the situation with regards to the tools. Respondents were presented with a list of tools and asked to check the ones they use in their practice.

Question 13

Respondents were then asked to state what influences the tools used. This in an effort to establish what factors influence the choice of the tools used.

The survey was sent to a group of known practitioners (control group of 15 practitioners) and then placed on the digital forensics forum (http://www.forensicfocus.com/) This forum was chosen because it is the premier online forum for digital forensics practitioners. The membership has been observed to include prominent digital forensic personnel. It was also added to two websites/blogs http://digiforensicsproject.webs.com/apps/links/ and http://digitalforensicsproject.blogspot.com/ as well as put up on Google plus https://plus.google.com/u/0/circles/forensic-consultants-p2e305db38e8bd342

3.3.1 Survey results

The researcher received ninety two responses to the survey however only eighty contained useful data. Six (6) of the respondents entered only their demographic data and left the other questions blank. Four (4) respondents answered only the questions marked compulsory while two were considered to be in sample errors because they were completed using random data that were irrelevant to the survey.

The survey sought to ascertain the diversity of the background of digital forensics practitioners. Results indicate that there are practitioners in the field from various different backgrounds. These include Law enforcement, Technical personnel (computer science/Information technology), Management (Business oriented), and Legal (Lawyers, solicitors, barristers).

Background of respondents	**%**	**Years in Practice**	**%**	**Students**	**Expert Witness**
Law Enforce	71	Under 1year	4	4%	53%
Technical	10	1-5	45		
Management	3	5-10	26		
Legal	3	10+	25		
Other	10				

Table 4.1 This table shows the background of participants in the study.

As indicated in table 4.1 above Seventy one (71) percent of the participants were of a law enforcement background, while ten (10) percent were of a technical (CS/IT) background constituting the majority of the sample. This distribution was deemed useful as it included personnel from the core areas representing the core facets of the digital forensics discipline. One of the pervasive issues with digital forensics is that often the investigation is conducted by persons not qualified in the field. Whereas it is widely accepted that due to the diverse nature of digital forensics there will be practitioners from varying backgrounds there is a basic level of qualification expected. Qualification in this sense refers to formal training in the area of acquiring digital evidence (digital forensics). The survey's indication of the majority of respondents being of a law enforcement background is not surprising as cybercrime is a criminal act and thus currently a number of police forces worldwide are instituting a cybercrime department and developing cyber related laws Met police (2012). This indicates an increase in efforts by different groups (governments and private sector) to fight the increasing occurrences of cybercrime worldwide.

The research sought to ascertain the relative level of experience that practitioners in the field, how long despite their background were they working as a digital forensics practitioner. Respondents were thus asked to indicate the number of years they had been practicing in the field, forty five (45) percent of the respondents indicated that they had been in the field for 1 – 5 years, twenty six (26) percent 5 – 10 years. Only four percent (4) of the respondents indicated that they had under four (4) years experience indicating that most of the respondents were experienced practitioners in the discipline of digital forensics. Additionally only four (4) percent of the respondents were students indicating that most of the respondents were practicing digital forensics personnel that had real life experience in the field. It is often argued that digital forensics is not necessarily for legal purposes however the term forensics suggests law and thus all digital forensics investigations should be carried out with the view that it may end up in court. From the survey the majority of the respondents (practitioners) fifty three (53) per cent were expert witnesses supporting the notion that the main objective of the digital forensic process is to acquire digital evidence for legal use.

Cyber crime has become widespread with recent surveys indicating that the top five countries for cybercrimes in 2011 were USA, France, Russia, Germany, and China (Europol). The data for 2012 showed the top three being Russia, China and South Africa respectively (Norton) This however did not present a clear reflection in the geographical location of respondents to the survey as instead of a list of individual countries, Europe was listed as a whole. The research sought to receive responses for a wide geographical area however sixty five (65) percent of the respondents were from Europe. Ten (10) percent of the participants indicated that they were from Asia, sixteen (16) percent from North America, six (6) percent from the Caribbean, and another six (6) percent from the Middle East. Whereas France and Germany could have been categorized as Europe while China may be categorized as Asia, there were no responses from Russia or from Africa to corroborate the results.

Digital Forensics is defined as “the science that is concerned with the relation and application of computers and legal issues” (Kutcha 2000). To ascertain the consistency in the concept of what digital forensics is and its definition in the field, question six on the survey questionnaire asked that each respondent define the term digital forensics. There were a variety of responses. Some respondents identified “digital forensics” as a science while there were others defined it as “an investigative procedure”. Other definitions included; One law enforcement personnel defined it as “finding evidence related to a crime that happened or investigating digital devices”. One private practitioner from Asia defined digital forensics as “the collection of evidence from digital devices”. One legal practitioner from the United States defined it as “the investigation of legal activity with the aim of providing related information or the identity of the criminal”. These varied responses to the question of definition highlight some of the inconsistencies in the field of digital forensics. It must however be noted that most respondents concurred that digital forensics involved the collection of data from digital/electronic devices and this is the definition employed throughout the project.

Literature reviewed and statistics published indicates that there has been an increase in cybercrime over the last decade (IC3) (Aeilts 2011). There have coincidentally been indications that there has been an increase in the request for digital forensics investigations in recent times. To quantify this assumption/observation the questionnaire sought to find out from practitioners the frequency with which their expertise was requested (question 8). The responses did suggest that there is indeed a widespread need for the use of digital forensics procedures, with responses ranging from daily, weekly, very often to “always have a backlog”. Forty percent of the respondents indicated that they had more than (20+) twenty request for digital forensics investigations in any given month.

One of the main objectives of the survey was to ascertain the current state of digital forensic procedures with regards to procedures used to carry out a digital forensic investigation and the existence or need thereof for standards in the field. Respondents were required to respond to questions attempting to ascertain if there were any particular procedure and/or policies in use within their organizations and if so, were there any policies in place to guide these procedures. This question was followed by another seeking to find out how the procedures (if any) were developed? The research also sought to ascertain if there were any particular tools favoured by practitioners and if so, what influenced the choice of tools.

	Yes	No
Are there policies in place to guide the Digital Forensic process	84%	16%
Were these policies…?	Percentage	
Developed in house	35	
Bought from a commercial organization	0	
Adapted from another organization/Body	13	
Other	52	

Table 4.2 This table shows how the policies are used by organizations are developed.

Where the researcher sought to ascertain if there were any policies in place to guide the digital forensics process eighty four (84) percent of the respondents said yes they had policies in place to guide the digital forensics process while sixteen (16) percent said no. This was an accurate reflection as it does show that there were policies used by some practitioners at some point during the digital forensics process. However in the follow up question where practitioners were asked how these policies came about thirty five percent (35) of the respondents said they developed them in-house, thirteen percent said they adopted them from other organizations and fifty two percent (52) responded by selecting other. The ad hoc way in which the digital forensics process is carried out was highlighted here. With thirty five percent of practitioners stating that they developed their own policies in-house it safely be interpreted that most practitioners do their own thing. This issue is collaborated by what was inferred by literature examined and statistical data.

Practitioners choosing 'other' indicated that the policies they used were based on those from other organizations and groups such as the Association of Chief Police Officers (ACPO), National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO) and The International Organisation on Computer Evidence.

These results confirmed the following: while there are policies in place to guide practitioners in the digital forensics process these policies are mainly developed by the organizations themselves with a lesser percentage being adapted from other organizations. This data highlights the ad hoc ways in which the process is carried out internationally. Organizations and individuals have their own guidelines that they create and adapt for use signifying that there is no one standard benchmark policy or guide that is used.

Respondents were asked if they used any particular methodology when conducting investigations of a digital forensics nature. The respondents indicated that they do not use any one specific methodology to acquire digital evidence. Twenty five (25) percent of the respondents answered yes while seventy five (75) percent indicated that they did not. Another attribute to the existing disjoint in the digital forensics field being the lack of uniformity in how specific tasks are carried out. Data here again indicates that practitioners in the field do their own thing, using their discretion based on a variety influencing factors

Respondents indicated that there were a variety of different factors dictating how an investigation took place and thus the methodology used was influenced by this. Influencing factors such as the type of investigation, who requires the investigation, the tools used were cited in addition to the issue of no particular methodology being in place that could be drawn on. An integrated methodology designed for use in varying circumstances involving different devices such as the one presented in this research will address this issue. This methodology is designed to accommodate different circumstances that may arise in a digital forensic investigation.

This ad hoc use of varying procedures throughout the digital forensics process was further highlighted when respondents were asked to list the steps taken to carry out the digital forensics process from start to finish. The responses were varied, with practitioners indicating different tasks that signalling the beginning of the process and varying tasks that indicated the end. While some practitioners saw their cases ending at the outcome of a case others saw it ending when they presented their report. There are some practitioners that respond to a request for their services by researching the background of the case, others had a preliminary look at the devices involved, while some practitioners indicate that the first step before doing anything was to ensure that they got legal permission. There was also wide variation with intermediate procedures taken throughout the digital forensics process. The ad hoc ways in which digital forensics is carried out has been an ongoing challenge for the digital forensic community. These challenges present issues with the robustness of the resulting digital evidence used in courts. There are a variety of tools available to help in the digital forensics process. The majority of these tools are open source and available free online while others are available commercially for a very high cost from vendors who drive the industry (Nance et al 2009). Such a variation in tool usage calls into question the issue of consistency and reliability. This is an issue that needs to be addressed in the field. To gather more insight on the methodologies used the researcher sought to find out if there was any consistency in the use of tools despite the wide availability of open sourced tools. The variance here was even wider as indicated in the chart below. Having presented what are deemed the more popular tools (based on widespread use) forty five (45) percent of the respondents chose "other", listing other tools such as Ufed and Paraben while thirty five (35) percent indicated that they used tools developed in house by their information technology departments. This is another indication of the existing inconsistencies within the field. Whereas there are a variety of digital forensics tools available worldwide there are still organizations and individuals who find it prudent to design and develop their own for personal/professional use. Popular tools internationally include Encase, FTK and Sleuth kit. The research further broke this data down to represent regions in an attempt to ascertain if particular tools were popular in particular regions. This was not so.

Tool	Caribbean	Europe	North A	Asia	Middle East
FTK	X	X	X	x	X
Encase	X	X	X	x	X
Sleuth Kit		X	X		

Table 4.3 Table showing the distribution of the use of tools worldwide

To address the issue of variance with regards to the use of particular tools this work includes the recommendation for use of particular tools based upon recommendations as indicated in Chapter 5 Section 2.

Which of the following tools do you employ throughout the investigation?

FTK	26%
Encase	35%
SIFT	3%
Sleuth Kit	16%
PTK Forensics	0%
The Coroners Tool Kit	0%
Open Sourced	29%
In house developed	35%
Other	45%

Nb. Respondents were allowed to select more than one checkbox, so percentages may add up to more than 100%.

Table 4.4 This table shows the percentage of respondents using particular tools. This list was compiled from a list of tools used by known practitioners.

The data collected revealed that Encase and FTK were the dominant tools used worldwide with Sleuth kit limited to Europe and North America. Respondents stated that their choice for any given tool is dependent mainly on cost, experience, recommendations from colleagues as well as that they kept using the tool they used when being trained as a digital forensics practitioner. Digital forensics commercial tools can prove to be very costly, (Austin 2007) and thus this is an important factor in any digital forensics practitioner choosing tools for practice. Practitioners like those in other fields are more comfortable using tools they are familiar with and thus will tend to stick to the tools they were taught to use during training (provided they did have specialized training in the field), this factor plays a great role in influencing the choice of tools.

The data gathered in this survey has indicated that digital forensics practitioners receive requests for digital forensics services daily while an investigation may last up to six months, sometimes more. This is due in part to a shortage of trained practitioners in the field (Bhaskar 2006) coupled with the large volumes of data that practitioners have to work with. Data gathered also indicate that there is a constant backlog of cases. These results confirm that there is need for improvement in the speed and efficiency in the way digital forensic investigations are carried out. This, while maintaining the integrity of the evidence found ensuring it conforms to legal and ethical standards because information gathered also show that eighty percent (80%) or more of the digital investigations carried out are eventually (if not initially) court cases with Seventy (70) percent of the respondents indicating that they were expert witnesses.

This section revealed particular issues with the digital forensics field. The results of the survey depict what was being suggested by the literature reviewed and added for insight into the research project as a whole. In summary the findings of the survey indicated that:

1. Digital forensics as a field was still in the developmental stages and there was still some work to be done to ensure that it becomes viable as a true forensics field.

While some progress has been made in the field over the past decade there is much more that needs to be done. (Garfinkel 2010) notes that there is much more that needs to take place in the field with regards to research and development.

2. There has been an increase in request for digital forensics investigations in the last decade.

With the increased use of technological devices, the need for digital evidence in a variety of cases has become paramount. This has in turn prompted the need for digital forensics investigations and investigators to acquire this evidence.

3. There are policies in place in most organizations to carry out the digital forensics process however they were either developed in-house or adapted from another, highlighting the issues of inconsistency and disjoint within the field.

4. There is no one methodology that is used as benchmark for digital forensics practitioners internationally. The use of a methodology is dependent on a number of factors including tools available, cost and the reason for the investigations.

5. The digital forensics field does not have an international set of standards that guide the investigative process of acquiring digital evidence.

There is no representative standardized benchmark methodology/model/process of acquiring digital evidence and thus organization and groups create their own. This ad hoc way of acquiring digital evidence introduces legal issues when this evidence is to be presented in the courts.

6. Personnel of different backgrounds including legal, managerial and academic are involved in the digital forensics field.

The field of digital forensics is diverse in that it encompasses different disciplines which are all integral to its operations. This has resulted in the field having practitioners from different backgrounds to address the needs of the field of digital forensics. This has resulted in the need for a set of guidelines and polices that address this diversity in backgrounds . 7. There are a number of practitioners in the field who attend court and/or support cases as expert witnesses in the field.

Like other forensics fields digital forensics practitioners are expected to present and explain his/her findings to a general audience in a way that is clear, concise and justifiable. Training and Education alleviates such issues and this research presents a curriculum that take into consideration the need for practitioners to be exposed to such training to be able to present and justify their findings in court.

In addition there are also a few questions arising from the analysis of these results:

1. How can time taken to complete a digital forensics investigation be reduced while retaining reliability in the results and their analysis?

The 2IR Mobile application developed to emulate the 2IR Methodology is designed to address this issue eliminating the need for bulky printed material providing built in legal and ethical guidance throughout the investigation.

2. Would a structured set of operating procedures help to reduce the backlog of digital forensics cases?

   The 2IR Framework of standards provides guidelines and principles for the 2IR digital forensics methodology which is a step by step description of carrying out the digital forensics process and addresses this issue. The 2IR designs presents a simplified and efficient way of performing the digital forensics process.

3. The majority of digital forensic evidence ends up in courts. Should the training of digital forensics practitioners not include all aspects of the investigations and not just the technical or legal areas? The development of a curriculum of studies encompassing all four core facets of digital forensics (legal, technical, educational, ethical) and including all aspects of a digital forensics investigation (from initiation to reporting) addresses this issue.

The development of an integrated methodology for the digital forensics process that incorporates the core facets of the field including education would help to alleviate the issues arising. The curriculum presented in Chapter five (5), Section three (3) incorporates subject matter that addresses all facets of digital forensics. This ensures that practitioners during training will be exposed to the different types of issues that they may face when carrying out their duties as digital forensics personnel.

The fundamentals of any digitally related criminal activity lies in "digital evidence". This evidence is acquired through the digital forensic process, which is an investigative process involving the collection, preservation, interpretation and presentation of evidence. This process as described may differ from one investigator to another despite the various legislations in place. A fact highlighted in the survey where respondents were asked to give their definition of Digital forensics. Digital evidence is unique in a number of ways based mainly on the form it takes which is not necessarily a physical one. (Mercer 2004) points out "if someone opened a digital storage device they would see no letters, numbers or pictures on it". The very nature of the data highlights the need for a digital forensic investigator to be thorough in carrying out their duties.

The term *Digital Evidence* is defined by (Casey 2011) as, "Encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator". The same term may also be defined to be, any data or information found to have been stored or transmitted in a digital form that may be used in court, (Hewling 2010). This type of evidence has become increasingly popular in recent years, as courts have begun to accept electronic based evidence for use in traditional cases.

As with any other type of evidence due diligence must be followed to ensure its reliability in a court of law and most courts have found it necessary to question the reliability of such evidence when presented. (United States v Carey and United States v Benedict).

This concern has been highlighted in several scenarios with the lack of standardization in the acquisition of digital evidence (i.e. Computer forensic methodologies) being blamed. (Casey 2004) supports this point stating, "Digital investigators do not have a systematic method for stating the certainty they are placing the digital evidence that they are using to reach their conclusions". The methodologies and tools used by digital forensic investigators worldwide have been variable and there is no one internationally accepted benchmark. (Casey 2004) continues, "This lack of formalization makes it more difficult for courts and other decision makers to assess the reliability of digital evidence and the strength of the digital investigators' conclusions". This dilemma is further supported by (Fulbright and Jowoski 2006) where they state, "The number one problem in current litigation is the preservation and production of digital evidence". The latter are two of the processes involved in the digital forensic process. The work presented in this project highlights how digital forensics investigative process can be standardized. By involving practitioners from different jurisdictions in its development and enabling contribution, from not only practitioners of different backgrounds, but also with different experiences from varying jurisdiction helping to place this methodology in the unique position of being used as an international benchmark for the field of digital forensics.

The problem of standardization in the area of digital forensics has been an issue from the initial stages and still faces major challenges when digital evidence is being presented in court. (See case Coleman Holdings Inc v Morgan Stanley). “Because computer forensics is a new discipline, there is little standardization and consistency across courts and industry” [USCERT]. It is integral that agencies and practitioners adhere to a defined set of standards and operating procedures to ensure this evidence and methodology is accepted by the legal community. Bryan Sartin, (Managing director of Cybertrust) in an interview with SCmagazine states that there is still much more to be done where digital evidence acquired through computer forensic is concerned. He noted that, “There are two things missing: a single commonly accepted standard and uniform code of working…. Quality of service across computer forensic providers varies dramatically …” (Chaikin 2007) sums up the need for standardization within the sector when he argues; “…there is an absence of generally recognized standards of best practice in digital evidence forensic procedures, and a lack of adequate training of forensic examiners”. He makes a very valuable point when he continues his argument, “errors in analysis and interpretation of digital evidence are more likely where there is no standard procedure for collecting, preserving and analyzing digital evidence”. Such statements from seasoned practitioners in the field highlight the need for standardization of the procedures used in the digital forensics field.

The need for standardization in the field has been duly noted and this need cannot be emphasized too much. This work presents a framework of standards incorporating principles from a/an educational, ethical, legal and technical perspective. These standards are designed to govern the field as a whole. To compliment this there is the developed methodology derived from the framework of standards as well as a curriculum of studies and a mobile application. These designs are all interrelated and thus present uniformity and consistency in the digital forensics field.

3.4 Summary

This research project was mainly qualitative (Grounded theory) but employed some quantitative methods (questionnaires). It was conducted in three main stages, (i) an initial survey of the existing literature in the field identifying any gaps and omissions following which the 2IR designs were developed. This was then followed with (ii) a gathering of data from practitioners in the field with regards to the initial design created and then finally (iii) the distribution of the designs for testing by practitioners in the field and interviewing of participants in the testing process. A discussion of the deliverables produced from various stages of the research and justification for their design are presented in the following chapters.

CHAPTER FOUR

The 2IR Framework and Methodology

This chapter provides a description of the 2IR deliverables, the 2IR framework, 2IR Methodology and a discussion of the data resulting from their testing by practitioners in the field. The need for standardization in the field of digital forensics cannot be overstated and thus the results of the survey served to inform the development of the 2IR framework, an accompanying methodology and mobile application. These designs were created with the objective of addressing the issue of consistency and cohesion within the field. The 2IR framework is a developed set of standards designed to govern the use of the 2IR methodology. The designs consists of three phases Initiation, investigation and reporting and four core areas as it relates to digital forensics (Legal, technical, education and ethical). The main aim is to bring coherence to the professional and occupational functions of the digital forensics field.

4.1 The 2IR Framework

This framework sets out and defines a set of characteristics that each practitioner carrying out an investigation should portray to enhance the validity of the digital evidence produced. It specifically addresses legal, technical, ethical and educational issues from incident response to reporting. The framework is arranged into three phases and four facets. One uniqueness of the framework is that there does not currently exist a framework in the field covering expected standards and with an accompanying methodology, as well as suggested tools and training curriculum that should have been covered by practitioners in the field. The 2IR framework addresses the core aspects of digital forensics, these are education, technical, legal and ethical (Craiger et al 2007). It draws on principles highlighted by different organisations addressing different aspects of the field. These include principles such as those developed by the Association of Chief Police Officers (UK), the Scientific Working Group on Digital Evidence and the Electronic Discovery Research Model (USA).

It presents a clear, concise, systematic and integrated approach to the digital forensics process. It incorporates additional integral domains to the digital forensics field such as chain of custody and educational background of practitioners that are critical to the presentation and admissibility of digital evidence in a court of law (Cohen 2008), (Casey 2011).

4.1.1 Core principles/Standards (general)

FRAMEWORK

Core Principles:

C1. Practitioners should be knowledgeable of the current legal requirements and policies impacting the investigation. [L/Ed]

C2. Practitioners should be trained and qualified in the area of digital forensics and handling digital evidence. [Ed]

C3. Two or more tools should be used in an investigation ensure accuracy of the results. [T/Ed]

C4. Practitioners should keep up to date with the developments in the field through training, workshops, conferences and research publications. They should evaluate their performance regularly and be committed to improving their practice through professional development and training. [E]

C5. Practitioners should have positive values and attitudes and adopt high standards of integrity in their professional role. [Ed]

C6. Practitioners should be familiar with a variety of operating systems. [T]

Figure 4.1 Core principles of the 2IR Framework

There are six general core principles governing the framework each of which is directly related to the four facets of the framework and the three outlined phases. These six principles were developed following careful perusal of existing related principles such as National Institute of Justice, Electronic Crime Scene Investigation: A Guide for First Responders, related Laws such as the Jamaica Cybercrime Act 2010, Malaysia Computer Crimes Act 1997, and general forensics standards such as Daubert/Frye Standards. They are:

i. legal;

ii. technical;

iii. educational;

iv. and ethical.

They also encompass the phases of the accompanying 2IR methodology developed as an accompaniment to the 2IR Framework, (i) Initiation, (ii)Investigative and (iii) Reporting. These core principles underpin all related principles in the 2IR framework. It is expected that practitioners should meet the listed core standards in their practice. All six principles are further expanded in detail in the facets. Additionally each facet has a set of at least four core principles directly related to that area and each phase has at least two core principles directly related to the phases. This along with more specific principles directly related to the facet and linked with the three phases formally identified as the standards in the framework are discussed in Sections 4.1.2, 4.1.3 and 4.1.4

4.1.1.1. C1. Practitioners should be knowledgeable of the current legal requirements and policies impacting the investigation.

Laws play an integral role in the process of digital forensics. Forensic science has its roots in law and is sometimes referred to as forensics which itself means the application of science to law (Walker 2007). The terms forensics and forensic science are often used interchangeably and both have become popular in many disciplines. Though forensics may be simply defined as the application of a scientific methodology in the legal system, (Casey 2004), outlines forensics as being "a characteristic of evidence that satisfies its suitability for admission as fact and its ability to persuade based on proof (or high statistical confidence)". Digital forensics is the branch of forensic science that has emerged to deal with the characteristics of legal evidence found in computers and other digital devices. (Nance et al, 2010) notes that the prevalent use of computers and its related digital technologies have become increasing popular. These devices have also been increasingly used to commit traditional crimes in new ways as well as to commit a whole new set of crimes. Digital/computer forensics emerged to address the investigation of and stemming the increasing occurrence of such activities. As with other forensics procedures digital forensics procedures are driven by applicable laws. These laws include those related to privacy, evidence and offences using and against computer related devices. These laws may be civil, criminal or administrative. A digital forensics practitioner must therefore be aware of the different laws applicable that play a role in the digital forensics process. This is especially important for specific laws addressing particular types of cases.

The practitioner also needs to be aware of outlined policies established in particular jurisdictions to guide the acquisition of digital evidence. Eg. ACPO (Association of Chief Police Officers Guidelines in the United Kingdom and the Scientific Working Group on Digital Evidence best practices for digital forensics (SWGDE draft best practices 2002).

Consideration must also be given to policies that may be present to govern particular processes within different organizations. It will be found that large organizations tend to have in house developed guidelines and policies developed for certain processes carried out within (eg Microsoft Inc). The policies will also have a legal bearing and thus legal counsel/guidance should be sought if this is so.

The legal issues surrounding the digital forensics process may be deemed overwhelming but should not be ignored as the majority of investigations end up in court. The laws must be strictly adhered to and chain of custody preserved. These legal issues are discussed in more detail in the legal section.

4.1.1.2. C2. Practitioners should be trained and qualified in the area of digital forensics and handling digital evidence.

Training is a critical issue in the field of digital forensics community as often practitioners are personnel from an organization's technical department. Training and qualifications are evidenced by a resulting diploma from the training organization. Additionally there are also professional qualifications such as The Certified Cyber Forensics Professional (CCFP) from $(ISC)^2$ Whereas lack of trained personnel has proved to be an important issue, this practice can present problems whenever a case is brought to court. Practitioners should endeavour to engage in a comprehensively developed education programme that integrates all aspects of digital forensics covering all disciplines involved, addressing the core problems facing the community such as reliability and consistency of the digital evidence produced. The current research has identified inconsistencies in the training of digital forensic practitioners as this is heavily driven by commercial companies that develop the requisite tools for investigating computer related crimes (Carlton 2007).

4.1.1.3. C3. Two or more tools should be used in an investigation to ensure accuracy of the results.

The 2IR framework principles dictate the use of at least two or more tools in mining, extracting and analyzing digital evidence. This is to ensure the validity of the evidence produced from the investigation. There are a number of tools available online (open-sourced and otherwise) that are used by digital forensic professionals worldwide. The choice of tools is usually dependent on personal preference, from experience or dictated by an employer or organization. Tools may be classified differently based on the focus of their use and their mode of availability as well as their relevance to the investigative process (Schatz 2007). There are those whose focus is on searching for the digital evidence while others are mainly used to preserve the evidence. Groups include; Multipurpose tools such as SANS Investigative Forensics Toolkit, Imaging Tools such as FTK Imager, Search Tools such as TCT-utils, Data Analysis Tools such as Backtrack, and Email analysis tools such as Mail

Viewer. Tools are discussed in further detail in the technical and educational standards section.

4.1.1.4 C4. Practitioners should keep up to date with the developments in the field through training, workshops, conferences and research publications (both industry and research led). They should evaluate their performance regularly and be committed to improving their practice through professional development and training.

Digital forensics is a subset of a very dynamic field and thus there are changes in the field quite regularly. An example is that of Apple (^{TM}) upgrading its products twice per year at times. Practitioners therefore need to ensure that they are constantly up to date with developments in the field and apply these developments to their practice. Constant training is critical to remaining current in the field. This 2IR Framework accompanied by methodology comes with a mobile application and has outlined in appendix C, a purpose designed curriculum for three levels, Certificate, Undergraduate degree and Post graduate degree. The integration of a research component moreso postgraduate helps to ensure that the curriculum is constantly updated and stays abreast with the changing technologies and current practice.

4.1.1.5. C5. Practitioners should hold positive values and attitudes and adopt high standards of integrity in their professional role.

Integrity and ethical behaviour are quite critical in the field of digital forensics. Integrity though lies in the personal moral background of the practitioner can be guided by dictated principles. Different organizations and groups have defined different ethical principles to guide their investigations such as the Association of Chief Police Officers. The 2IR frame work has defined ethical principles to guide the accompanying methodology. These principles are outlined in the framework generally, while there are outlined principles for each section and phase. These have been developed after careful perusal of existing ethical guidelines in place for various professionals in different organisations such as the operational principles of police forces, legal and ethical principles of law firms, operational principles, guidelines and standards for education professionals.

4.1.1.6. C6. Practitioners should be familiar with a variety of operating systems.

There are a various operating systems that drive different digital devices. Practitioners in the digital forensics field need to have training and experience in using different operating systems. The field of digital forensics includes mobile forensics, network forensics, and cloud forensics. Additionally, considerations need to include developments such as the Internet of Things (IoT), The concept of Bring Your Own Devices (BYOD) and the generally interconnectivity of devices used within the environment. This current scenario reinforces the need that a digital forensic practitioner's knowledge base regarding operating systems needs to be wide. Operating systems including, but not limited to, Andriod, iOS, Windows X, Mac OS, Linux, and Unix for example.

The core principles/standards are the principles that are do not fall within the remit of any particular phase or facet. They are general and have been designed to set out the fundamental operating parameters within which all digital forensic practitioners should operate whatever their point of entry into the field. These standards outlined indicate activities critical to the continuous improvement of practice outlining areas where the practitioner should be able to assess their own practice, receive and employ valuable feedback from colleagues. As a practitioner's career progresses it is expected that they will extend the dept and breadth of their knowledge, skills and experience and demonstrate this in the context in which they practice.

4.1.2 Core Principles -The Phases

The framework also includes core principles directly related to the three phases of the framework. These three phases are directly related to the phases of the 2IR methodology.

They are:

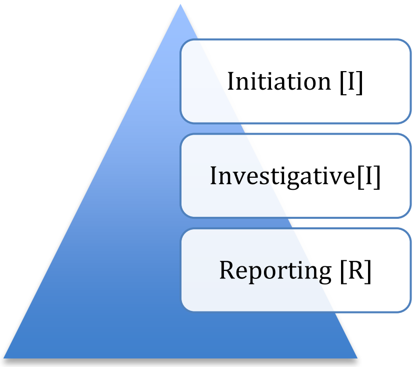


Figure 4.1 1 Phases of the 2IR Framework (Phases of the Digital Forensics Process)

The main aims and core principles of the three phases of the 2IR methodology and framework are described below.

Initiation

Aim: To set the stage for an investigation that will produce digital evidence that is legally admissible in a court of law.

The standards outlined in this phase serve to guide practitioners in preparing all the documentation needed to ensure a productive and successful digital forensic process. These standards cover the all the facets with regards to the initiation phase.

Core standards directly related to the initiation phase are as follows:

Initiation
(I_1)

$I_1$1. Practitioners must observe the legal requirements for the authorization and capture of digital evidence.
$I_1$2. Practitioners must be cognizant of the expectations of all stakeholders.
$I_1$3. Establish a chain of custody and the reporting format for tasks.

Figure 4.2 Core Principles of Initiation Phase

$I_1$1. Practitioners must observe the legal requirements for the authorization and capture of digital evidence.

Authorization such as a warrant is quite critical to any investigation and the presentation of evidence from that investigation. It is important that proper authorization to search and seize are received as failure to do so can result in problems when evidence is to be presented. The field of digital forensics like other forensics fields must be guided by law and thus careful legal adherence must be maintained. Legally acceptable authorization such as a warrant must be obtained before the acquisition of digital evidence begins. The search warrant is required to search and seize in most jurisdictions including The United States, Caribbean and Europe.

Obtaining a search warrant is itself subject to particular requirements that a practitioner must also be knowledgeable of.

$I_1$2. Practitioners must be cognizant of the expectations of all stakeholders.

It is during this phase that the digital forensic practitioner/forensic team should establish the expectations of all stakeholders. It is important to ascertain exactly what will be expected of the team and ensure that delivery of such is possible. This may be done using mini interviews with stakeholders using questions such as those suggested on form IA1 in the appendix C. Practitioners must ensure that the objectives of the investigation are the same from both the perspective of the investigating team and the requesting party.

$I_1$3. Establish a chain of custody and the reporting format for tasks.

Chain of custody is important to the presentation of legal evidence and this must be observed throughout the entire process starting at the very first phase. Chain of custody is the process of validating how the evidence is gathered, tracked and maintained while it is collected. This chain of custody supported by an established reporting format for tasks (such as those presented in appendix D) can prove very critical especially if practitioners are required to be expert witnesses in a case. A poorly undertaken chain of custody or not doing having a chain of custody can present issues with the presentation of the evidence in a court of law. See cases (Zubulake vs. UBS Warbug 2003, American Express Inc vs. Vee Vinhee 2005).

Investigative

Aim: To produce digital evidence that is able to withstand the rigors of a court of law. The methods used to produce this evidence should produce the same results if used by another practitioner.

The standards in this phase serve to guide practitioners throughout the investigative phase of the digital forensics process. It helps to ensure that intricate steps in the process including copying, preserving, mining and analyzing digital data are carried out accurately. These phases are very important to the presentation of the digital evidence that will be found and thus must be carried out under the observance of principles and standards put in place.

Core principles directly related to the Investigative phase

Investigation

I_2

$I_2$1 Practitioners must adhere to guidelines to ensure sound retrieval of digital evidence.

$I_2$2 Practitioners must observe techniques to ensure preservation of digital evidence before, during and following acquisition.

$I_2$3 Practitioners must ensure correct measures are taken to protect the scene of the incident.

Figure 4.3 Core Phases of the Investigation Phase

$I_2$1. Practitioners must adhere to guidelines outlined in the 2IR Framework and accompanying 2IR Methodology to ensure sound retrieval of digital evidence.

It is important that digital forensics practitioners follow all stipulated guidelines when retrieving digital evidence from electronic devices. These guidelines whether internal to organization, national or international policies should be adhered to or could result in legal problems in the investigated case should it go to court. Practitioners must also observe techniques to ensure preservation of digital evidence before, during and following acquisition. Preservation of digital evidence is key to all digital forensics investigations. Documented techniques exist for the preservation of digital evidence at all stages throughout the process [see 2IR Methodology – Section 4.2] and practitioners are all expected to know and observe these techniques as stipulated. This to ensure that the digital evidence acquired is robust enough to stand up in court.

$I_2$2. Practitioners must ensure correct measures are taken to protect the scene of the incident.

Sanitation of an incident scene is important and thus it needs to be protected from contamination. This, in the sense that data can be changed intentionally or otherwise and thus all precautions must be taken to prevent this happening. Guidelines to ensure that such a situation does not occur is incorporated and outlines in the 2IR Methodology presented in Section 4.2. This can be especially difficult when dealing with computers and related devices. Keeping persons away from a physical scene is one thing however a digital crime scene may involve networks connecting to computers in various locations including the cloud, (Casey 2004).

$I_2$3. Practitioners should maintain a chain of custody.

Digital forensics practitioners should endeavour to keep a detailed record of all activities that they carry out during the investigative process. (Chisholm 2010) states, “Forensic analysts should always keep detailed logs of the actions they perform through the acquisition and collection process”. (Investigative stage in the 2IR Framework) This is critical to all stages of the investigation more so the investigative phase as these help to prove that there was consistency throughout. These may be in the form of paper logs or electronic but it should be producible upon request. Chain of custody may be used along with hashing to indicate that integrity was maintained throughout the process and should be maintained through the entire process. The importance of the chain of custody cannot be overestimated as duly noted by Case 2004, “one of the most important aspects of authenticating is maintaining and documenting the chain of custody of evidence”. Maintaining the chain of custody is also important as anyone who handles the evidence may be required to appear in court as an expert witness.

Reporting

Aim: To produce a comprehensive report of findings. A report that is comprehensive to all personnel involved including those from non technical fields.

This is the final stage of the digital forensics process as per 2IR methodology. The standards here outline the principles for guiding the practitioner in pulling together all the electronically stored information that was identified, preserved and analysed for presentation to a court of law. The objective most times is to prove or disprove a fact and thus the practitioner must be prepared to stand by the findings presented.

Core principles for the reporting phase

Report
(R)

R1. Practitioners should ensure accuracy in classifying and reconstructing the incident scene.
R2. Practitioners should be constructive in producing a relevant report.
R3. Practitioners should recognize that this phase may include being an expert witness.
R4. Practitioners should be reflective and responsible for identifying drawbacks and facilitate ways for improvement.

Figure 5.4 Core Principles of the Reporting Phase

***R1.* Practitioners should ensure accuracy in classifying and reconstructing the incident scene.**

Reconstruction of the incident scene is critical in identifying exactly what happened, when it happened and where exactly it happened. Casey 2004 notes that reconstruction of the incident scene leads to a more complete picture of the incident. All this combined will point in the general direction of who exactly was involved. Accuracy in reconstruction of the incident scene helps in alleviating any vagueness in the analysis of the data reducing erroneous conclusions. Guidelines to reproducing an incident scene is further discussed in section 4.2, The 2IR Methodology with example forms of how to do this is presented in appendix C.

R2. Practitioners should be constructive in producing a relevant report.

Presenting digital evidence retrieved from the digital forensics process can present a challenge even to the more experienced, however it is very important that all reports produced whether electronic or otherwise are constructive to the reader as well as relevant to the specific case. Specific guidelines to producing such a report are detailed in section 4.2, the 2IR Methodology with samples in appendix C.   It is helpful to produce the report/s based on the original objective/s of the case. The objectives and findings should correlate and any additional findings in the report should be thoroughly explained and justified by the practitioner.

R3. Practitioners should recognize that this phase may include being an expert witness.

An Expert witness, sometimes referred to as a professional witness, is someone who is deemed to be an expert in a particular field and is at times required to provide their technical or scientific opinion about evidence produced themselves or other experts in court. Part of the reporting phase may or may not include such a presentation, but it is quite possible it will. This is the stage where the authenticity of the evidence will be queried and practitioners must be prepared to establish its reliability and robustness to ensure admissibility. It is important to note that at this stage the integrity of the practitioner is also at stake and thus honesty and consistency are very important factors.

R4. Practitioners should be reflective and responsible for identifying drawbacks and facilitate ways for improvement.

During the reporting phase is where all information/data/evidence collected is collated and put into a meaningful format. This is therefore a time when the practitioner can reflect on how the entire process was carried out, where the good and not so good points can be highlighted, and steps taken to ensure that such poor practice is not repeated. During the phase the practitioner should note ways to improve the process and ensure dynamicity and currency. Dynamicity and currency in the field may be achieved through attendance and participation in courses, workshops, conferences and reading digital forensics related communications such as journals including; The Journal of Digital Forensics Security and Law, International Journal of Electronic Security and Digital forensics and International Journal of Cyber-Security and Digital Forensics.

Summary

The core principles of the 2IR framework as they relate to a specific phase have been designed to outline the basic operating parameters within the phase. These operating parameters are not specific to any of the core facets outlined in the framework but spread across all, and are specific only to the phases in which they are listed. These principles reflect the basic expectations of a practitioner functioning at each phase.

4.1.3 The Facets

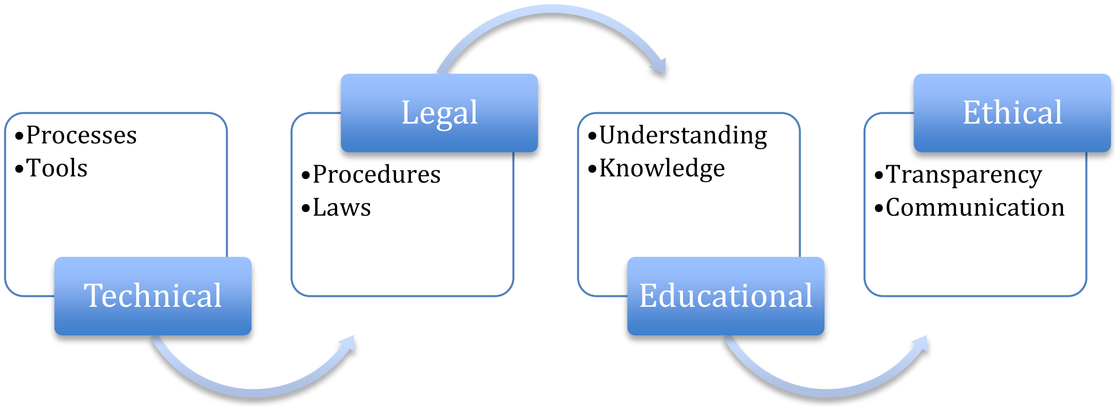
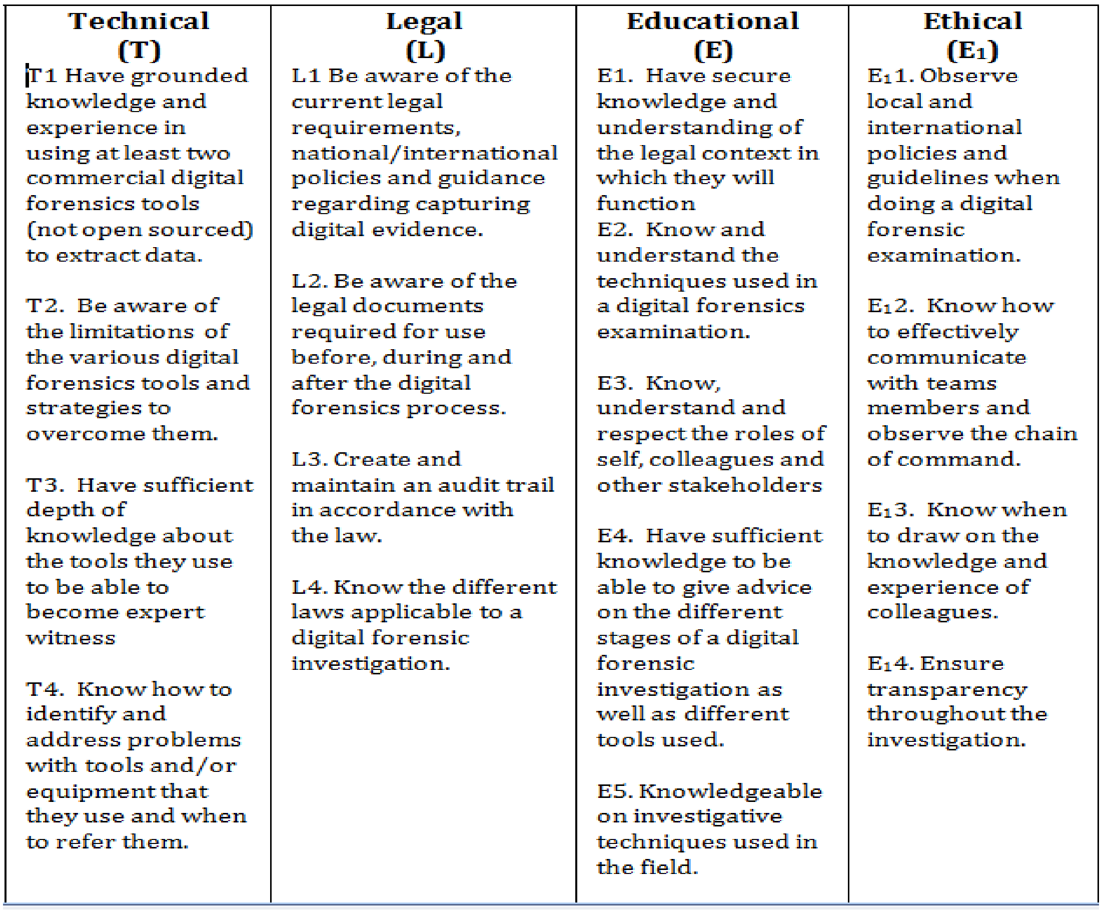


Figure 4.5 Overview of the facets of the framework

Each phase in the 2IR framework falls into one of the four facets of the framework. These facets represent the different fields embedded in digital forensics. They are legal, technical, educational and ethical, (Craiger et al 2007) it is under these facets that the standards governing the 2IR methodology are framed.



Technical (T)	Legal (L)	Educational (E)	Ethical (E_1)
T1 Have grounded knowledge and experience in using at least two commercial digital forensics tools (not open sourced) to extract data. T2. Be aware of the limitations of the various digital forensics tools and strategies to overcome them. T3. Have sufficient depth of knowledge about the tools they use to be able to become expert witness T4. Know how to identify and address problems with tools and/or equipment that they use and when to refer them.	L1 Be aware of the current legal requirements, national/international policies and guidance regarding capturing digital evidence. L2. Be aware of the legal documents required for use before, during and after the digital forensics process. L3. Create and maintain an audit trail in accordance with the law. L4. Know the different laws applicable to a digital forensic investigation.	E1. Have secure knowledge and understanding of the legal context in which they will function E2. Know and understand the techniques used in a digital forensics examination. E3. Know, understand and respect the roles of self, colleagues and other stakeholders E4. Have sufficient knowledge to be able to give advice on the different stages of a digital forensic investigation as well as different tools used. E5. Knowledgeable on investigative techniques used in the field.	$E_1$1. Observe local and international policies and guidelines when doing a digital forensic examination. $E_1$2. Know how to effectively communicate with teams members and observe the chain of command. $E_1$3. Know when to draw on the knowledge and experience of colleagues. $E_1$4. Ensure transparency throughout the investigation.

Figure 4.6 The core principles of the facets (The entire framework as a whole can be seen in appendix E)

The technical facets cover the tools and process, the legal facet covers the procedures, laws and guidelines. The educational facet covers knowledge, training and understanding while the ethical facet looks at transparency, communication and basic morals concerned with operating in a forensics field.

4.1.3.1 Ethical

Ethical standards are the statements of a practitioners professional attributes that are expected to be maintained throughout their career.

These standards are developed to be meaningful to the practice of digital forensics . Their main purpose in the framework is to:

1. inspire practitioners to reflect and uphold the integrity of the profession;
2. guide ethical decisions in the field;
3. specify ethical responsibilities in digital forensics practice;
4. promote trust and confidence in the field of digital forensics.

Core Principles/Standards

The Ethical Principles (E_1) principles set out aspirational guidelines intended to serve as a source for ethical decision making by practitioners in the digital forensics field. Developments of these principles were guided by the Electronic Discovery Reference Model for the e-discovery field (http://www.edrm.net/) as well as the Association of Chief Police Officers Good Practice Guide for Computer Based Electronic Evidence (http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf). The 2IR E_1 principles consist of four main principles as well as sub principles covering each phase. These principles are intended as a guide to the ethical conduct of practitioners in the field. They represent general standards which each practitioner needs to meet upon becoming a digital forensics professional. Where as it is expected that each individual case will vary in its requirements, as will the evidence examined so is it expected that no specific set of rules or guides will fit all occasions. However the policies and standards stated in this document are to be seen as indicating the conduct requirements expected by practicing digital forensics practitioners. Failure to maintain minimum standards will cast some doubt on the practitioners suitability for the field of digital forensics. This point is reinforced by (King 2006) who notes that nothing can replace integrity and high moral standards in professional practice.

$E_1$1. Observe local and international policies and guidelines when performing a digital forensic examination.

Policies are critical to the digital forensics field. Forensics is deeply intertwined with law and policies in the field are created based on the 'rule of law". Policies and guidelines are put in place to describe best practices in a particular field, clarify principles and guide particular processes. Policies describe standards that practitioners in a field should follow when carrying out their duties. An example of existing standards and guidelines established in the field includes that of the Association of Chief Police officers (ACPO) good practice guide for digital evidence. To this end practitioners must endeavour to know the legal framework in which they operate whether they be local and/or in-house or national policies.

$E_1$2. Know how to effectively communicate with team members and observe the chain of command.

Communication is important to any investigative process. Whether a practitioner is working alone or with a team, communication is integral between all stakeholders. Practitioners must be aware of the chain of command that exists during all investigations. The practitioners must know who to contact in the event of any issues regarding particular aspects of the process. This also helps to maintain communication with all stakeholders throughout the digital forensics process. It is also integral that all expectations are known and made clear as well as constantly updated throughout the investigation.

$E_1$3. Know when to draw on the knowledge and experience of colleagues.

The digital forensics process can be especially complicated if working as an individual practitioner. Practitioners thus must be cognizant of the fact that there will be times when additional expertise may be required. Practitioners should endeavour to keep up to date with developments and at the same time they need to know their weaknesses/limitations and be able to recognize when additional expertise is required.

$E_1$4. Ensure transparency throughout the investigation.

A critical part of integrity as a profession is embedded in transparency. Transparency may be described as lacking of a hidden agenda and conditions, accompanied by the availability of full information required for collaboration, cooperation and collective decision making and "Minimum degree of disclosure to which agreements, dealings, practices and transactions are open to all for verification". This description of transparency suggests that procedures being used should be 'above board'. They should not only be in accordance with law but applicable and relevant. All stakeholders should be aware of what is being undertaken. At any point during the investigation, if asked the practitioner should be able to provide information on the tasks and procedures being employed. The practitioner should ensure transparency by keeping all stakeholders in the "loop". It should be easy to identify what is taking place throughout the digital forensics process. The process should not be secretive, openness and effective communication is essential.

4.1.3.2 Technical

Technical Standards outline the technical guidelines encompassed in a digital forensics investigation.

The technical standards define the basic technical expertise of a digital forensics investigator. It outlines the use of tools and the procedures associated with the process.

Core principles (T)

T1 Have grounded knowledge and experience in using at least two general commercial digital forensics tools (not open source) to extract data.

The technical/scientific aspects of digital forensics is critical to any related investigation. Without technical knowledge of the processes involved, the tools and the devices to be investigated there is not much that can be done. The 2IR system recommends that at least two (2) tools be used in any investigation; as such it is expected that each practitioner will be proficient in using at least two general commercial tools.

T2. Have sufficient in-depth of knowledge about the tools they use to be able to become expert witness.

Forensics practitioners are at times required by the court to explain their findings, procedures and tools. Practitioners should know the tools they have been trained to use very well. They should be able to use these tools appropriately and describe how they work to what they do should the circumstances arise. The practitioner is expected to have specialized knowledge with regards to the tools they use and be able to describe related processes, policies and procedures. They should be aware of exactly what the tools do, how they do it what their results should look like and thus be able to explain this so that persons outside the filed are able to understand.

T3. Be aware of the limitations of the tools they use.

There are a number of tools available some open sourced, free and other commercial. Examples of some available tools include, but aren't limited to, Encase by Guidance Software, Forensic Toolkit (FTK) by Access Data and Win Hex by X-Ways Software Technology. Practitioners need to be aware of any limitations that exist with the tools they use. A practitioner is not expected to know all existing tools but for the ones that they are trained to use it expected that they will be aware of any limitations in its use and how it may have impacted the digital evidence produced. They should be aware of exactly what the tools do what their results look like and thus be able to explain this to a layperson and also to be able to identify whenever the tool is not working as it should.

T4. Know how to identify and address problems with tools and/or equipment that they use and when to refer such issues to another party.

This standard is closely linked with T3. Along with knowing the limitations of the tools they work with, practitioners should also be able to identify when any problems arise with functioning of the tools that may affect the resulting digital evidence produced. Practitioners also need to be able to identify when there is an issue arising that is directly related to the use of the tools and be able to address them or refer to appropriate personnel.

4.1.3.3 Educational

Educational Standards clarify the basic educational background (For example degrees in the field) and training (for example professional training such as Certified Hacking Forensics Investigator) that digital forensics practitioners at different levels should portray.

These standards define the knowledge and skills that practitioners should posses. It also encourages the highest qualification possible in the field. It also indicates the different professional training that is relevant and widely acceptable in the field. The Education standards are a guide to the relevant basic information and knowledge a practitioner in the field should possess.

Core principles (E1)

E1. Have grounded knowledge and understanding of the legal context in which they will function.

Digital forensics is grounded in law and this facet is just as important as the others in which the field operates. Practitioners must be cognizant of the legal impacts of their field. They must be knowledgeable on the law as it relates to digital forensics. Whereas they are not expected to have legal training they are expected to have a significant amount of knowledge in the legal area. This knowledge is to be gained from a relevant and valid training course and thus any course purporting to be training and education in Digital Forensics (Such as presented in Appendic C) should include a module on the relevant laws.

E2. Know and understand the techniques used in a digital forensics examination.

Practitioners are not only expected to know the process but to understand what they do. Practitioners are expected to understand the techniques they use to uncover digital evidence enough to be able to explain it and know when things are "off". A relevant and valid course in pursuit of digital forensics education would include content on the techniques (technical and otherwise) used in the Digital Forensics process. Relevant training in the field would assist practitioners in being able to interpret any discrepancies that may occur. Knowledge of the standard investigative techniques would also be required in addition to other technical knowledge.

E3. Know, understand and respect the roles of self, colleagues and other stakeholders.

Practitioners need to understand their general roles as a digital forensics practitioner as well as their roles in specific cases. They need to be clear on the chain of command in the environment in which they work and observe them. It is wise to be aware of the roles of colleagues, thus knowing the boundaries of each role. It is expected that before becoming a practitioner an individual would have been exposed to the different roles encompassed in being a practitioner in the field.

E4. Have sufficient knowledge to be able to give advice on the different stages of a digital forensic investigation as well as the different tools used.

Knowledge of the field of operation is key and cannot be over emphasized. As a forensics practitioner one is expected to have specialized knowledge by virtue of education and training being able to give insight and advice when needed. This is especially vital when working with private organizations as the practitioner will be expected to be able to effectively advise and provide rationales for the steps taken.

E5. Knowledgeable on investigative techniques used in the field.

In addition to the technical and legal knowledge required the digital forensic practitioner must be cognizant of the investigative aspect of the field. There may be times when a practitioner will be working along with law enforcement that are trained investigators and thus some skills fundamental to this aspect of the field will be required. There will also be times when practitioners will work as a team with other practitioners, at these times practitioners will need also need to be aware of different investigative techniques.

4.1.3.4 Legal

Legal standards indicate the legal aspects of the investigation that must be observed by the digital forensics practitioner.

These standards outline the legal requirements of a digital forensics investigation. It also lists the related laws to be observed during the different phases of the investigation

Core Principles (L)

L1 be aware of the current legal requirements, national/international policies and guidance regarding capturing digital evidence.

The legal context in which a digital forensics practitioner operates cannot be overstated. The practitioner, though not expected to be a legal expert, must be familiar with the current legal requirements for the job. National and international policies that are founded on the rule of law must be followed. There are formally accepted international benchmark principles however principles such as those from ACPO and SWGDE or other developed in different jurisdictions should be observed. Laws, policies and guidelines are changed and updated quite often and thus practitioners must be aware of any changes that may occur.

L2. Be aware of the legal documents required for use before, during and after the digital forensics process

As with any forensics field there will be a number of documents required for completion to ensure the chain of custody is preserved. Practitioners must be knowledgeable about the various forms such as a warrant that are required of the investigation. The legal facet is further expanded in Section 4.2 with samples of such documents are presented in appendix D.

L3. Create and maintain an audit trail in accordance with the law.

It is important in any investigation that has the possibility of ending up in court that an audit trail is created and maintained. This is done with the aid of the documents mentioned in L2. (for example Phase completion forms and Evidence collection forms) It is essentially a chronological record signed and dated by the practitioner that list all activities that took place throughout the digital forensics process.

L4. Know the different laws applicable to a digital forensic investigation.

As alluded to in the core principles governing the framework there are particular laws that are applicable to the digital forensics process. The practitioner must be cognizant of these and ensure that there is adherence to them throughout the process.

Section 5.3 -The 2IR Application presents a programme to guide the practitioner through the digital forensics investigative process assisting with adherence to rules and guidelines presented in the 2IR Framework and Methodology (Section 4.2)

The standards/principles outlined in this section represent the basic operating parameters in which a digital forensic practitioner will function as it relates to the facets of digital forensics. It sets out the basic operating environment and expectations as it relates to the facets of the field and is not limited to any particular phase of the investigation.

4.1.4 Section Principles

Technical (T) ***Tools and Procedures***	***Legal (L)*** ***Procedures***	***Educational (E)*** ***Certifications and qualifications***	***Ethical (E1)*** ***Roles and responsibilities***
$TI_1^{(1)}$ Know the range of devices that may be involved in the investigation. $TI_1^{(2)}$ Select appropriate tools based the digital devices to be encountered in the investigation.	$LI_1^{(1)}$Aware of legal requirements for the capturing of digital evidence. $LI_1^{(2)}$ Select tools for the investigation in accordance with the recommended principles and guidelines.	$EI_1^{(1)}$Posses the educational background and capability to handle all aspects of the investigation. $EI_1^{(2)}$ Select tools that the practitioner has been trained to use.	$E_1I_1^{(1)}$Disclose any conflict of interest with regards to the impending investigation. $E_1I_1^{(2)}$Approach the investigation objectively.
$TI_2^{(1)}$Appropriate methods and techniques are used in accordance with the recommended guidelines. $TI_2^{(2)}$Ensure tools used are clearly understood and can be used by another investigator and produce the same results	$LI_2^{(1)}$Ensure that methods used can be reproduced by other investigators producing the same results. $LI_2^{(2)}$ Be aware of the laws associated with the investigation at this stage. $EI_2^{(3)}$Treat all data and devices as potential legal evidence.	$EI_2^{(1)}$Ensure that practitioner is trained to use the tools available where open source or commercial. $EI_2^{(2)}$Ensure knowledge of the different tools to be used for different purposes throughout the examination. $EI_2^{(3)}$Treat all data and devices as potential legal evidence. $EI_2^{(4)}$ Be Knowledgeable of the tools they work with and how they do what they do.	$E_1I_2^{(1)}$Maintain objectivity throughout the investigation $E_1I_2^{(2)}$Treat all data and devices as potential legal evidence. $E_1I_2^{(3)}$Exercise care to ensure to ensure the integrity of the evidence acquired. $E_1I_2^4$ Ensure validity and reliability in the materials analyzed.
TR^1 Archive all software tools used. TR^2 Archive all hardware tools used	LR^1 Document all hardware tools used in accordance with the recommended guidelines. LR^2 Document all tools in accordance with the recommended guidelines LR3 Regardless of legal definitions, a digital forensics practitioner will realize that there are degrees of certainty represented under the single term of expert opinion. The practitioner will not take advantage of the general privilege to assign greater significance to an interpretation than is justified by the available data.	ER^1 Practitioners must have sound knowledge in the reconstruction of a digital crime scene. ER^2 Practitioners must be knowledgeable in archiving and documenting tools used ER^3 Practitioners must adequately trained to produce a comprehensive report of the investigation. ER^4 Posses training to interpret findings accurately ER^5 Be knowledgeable in creating an attacker profile.	$E_1R^{(1)}$ Practitioners must ensure confidentiality in the findings of the investigation. $E_1R^{(2)}$ Practitioners must ensure full disclosure of their findings to the relevant personnel. E_1R_3 When a practitioner works as an expert witness they will not take advantage of the privilege to express opinions by offering opinions on matters within their field that is not necessarily their area of expertise. E_1R_3 Conclusions should not be drawn from materials that atypical and/or unreliable. E_1R_4 Where results are inconclusive or indefinite any conclusions drawn should be fully explained in the report.

Figure 4.7 Principles in the different phases and facets of the 2IR framework (see full framework in appendix)

The principles outlined in the framework of standards are further arranged based on the phase in which they are most relevant and under the particular facet to which they apply. For example Standard E^1R^4 would be relevant to the reporting phase but falls within the remit of the Ethical Facet. Each section of the framework has at least two standards which apply.

Initiation Phase -Technical

The principles outlined here detail the standards to guide digital forensics examiners as it is related to the technical aspects of the initiation phase of the framework. They serve to guide the practitioner as to the basic technical foundations required to be a digital forensics practitioner.

$TI_1^{(1)}$ Know the range of devices that may be involved in the investigation

Practitioners must identify, during this phase, the devices that will be required for use throughout the investigation. They must be cable of stating the range of devices involved (i.e whether they will be working with, desktops, laptops and/or mobiles etc). This is because cases may require specific expertise in a particular area and specific tools for particular devices.

$TI_1^{(2)}$ Select appropriate tools based on the digital devices to be encountered in the investigation.

Practitioners must be cognizant of the different tools available to be used with different devices. Some tools will not be a one-size fits all and thus practitioners must be aware of this. There are a variety of tools developed to address different technological devices. Additionally one may decide to specialize in a particular aspect of digital forensics such as cloud forensics or mobile forensics.

Initiation Phase – Legal

The principles outlined here are standards to be observed that are specific to the initiation phase but fall into the legal realm of the framework. They serve to guide the practitioners on the legal principles that must be observed when carrying out a digital forensics investigation.

$LI_1^{(1)}$Be aware of legal requirements for the capturing of digital evidence.

Evidence is critical to any forensics process and thus care must be taken in the process of acquiring it. Evidence in a court of law is usually the deciding factor in the outcome of a case and thus it is important that at this phase the practitioner starts off in the correct mode by being cognizant of the legal requirements both in-house and as it relates to the jurisdiction in which one operates for capturing evidence and more directly digital evidence.

Practitioners must be aware of the legal constraints at this stage. This is the initiation phase and thus all legal factors must be considered before the actual investigation begins. Legal documents, consultations with the legal team and legal authorization to actually carry out the investigation must be completed during this phase

$LI_1^{(2)}$ Select tools for the investigation in accordance with the recommended principles and guidelines.

Principles and guidelines are the hallmarks for legal guidance in organizations and must be adhered to. Along with legal statutes put in place nationally and internationally practitioners must be cognizant of principles within an organization that may be legally binding. Practitioners must ensure that they find out about any internal policies in place within the requesting organization that may impact on the process of digital forensics. Going against the embedded principles within an organization may result in a whole new set of legal issues or a case within itself.

4.1.4.2 Initiation Phase – Education

The principles outlined here are standards to be observed that are specific to the initiation phase but fall into the education realm of the framework. They serve to guide and inform practitioners of the basic educational requirements needed to be successful in the digital forensics field as it relates to the initiation phase.

$EI_1^{(1)}$Posses the educational background and capability to handle all aspects of the investigation.

Education is critical to all forensics fields and to all phases. At this phase the practitioners needs to ensure that before they take on the task, all the required skills and educational background and training are in place. If the practitioner is working as a part of a team it is important that the team members possess the required skills needed to carry out the entire investigation throughout all phases. If working as an individual, the practitioner should ensure that he/she has the required skills to carry out the entire process. Qualifications such as a certificate or degree in information security and/or digital forensics along with or professional qualifications for example Certified Ethical Hacker (CEH) and/or Certified Hacking Forensics Investigator (CHFI).

$EI_1^{(2)}$ Select tools that the practitioner has been trained to use.

Tools are the main components of any digital forensic investigations and thus practitioners must be adequately trained to use various tools applicable to different sections of the investigation. Practitioners should receive training in using at least three different tools. It is recommended that while practitioners may be experienced using a variety of open source tools they be formally trained to use at least two commercial tools, such as Encase by Guidance Software and P2 Command Kit by Paraben Corporation.

4.1.4.2 Initiation Phase – Ethics

The principles outlined here are standards to be observed that are specific to the initiation phase but fall within the ethical realm of the framework. They serve to guide the practitioner as to the particular ethical behaviour that is expected of practicing forensic professionals.

$E_1I_1^{(1)}$Disclose any conflict of interest with regards to the impending investigation.

Ethical behaviour is critical to the practice of any forensics practitioner and their practice. It is during this phase that the practitioner must ensure that the case doesn't conflict with anything personal or any other case that is being, or has been worked on. The practitioner should check to ensure that there is no influence that would create a risk to his/her professional judgment or actions throughout the case.

$E_1I_1^{(2)}$Approach the investigation objectively.

Objectivity is important in all investigations and thus the practitioner must approach all cases with an open mind. The practitioner should endeavour to use only the information captured during a phase to carry out the investigation, and not allow issues from previous investigations and other outside influence to affect the investigative process. Whereas personal experience in any field is valuable it should not promote prejudices or encourage one to be judgmental in making decisions related to a case.

Summary

This section outlined the standards within the Initiation phase as they fall under the different facets. These are principles directly related to the initiation of the digital forensics process, they address processes and tools under the technical facet, procedures and law under the legal facet, understanding and knowledge under the educational facet while transparency and communication are addressed under the ethical facet. These principles are critical as they set the stage for the successful acquisition of digital evidence that may be used in a court of law.

4.1.4.3 Investigation Phase – Technical

The principles outlined here are standards to be observed that are specific to the Investigation phase but fall in the Technical realm of the framework. They serve to guide the practitioners about the technical requirements for this stage of the process.

$TI_2^{(1)}$Appropriate methods and techniques are used in accordance with the recommended guidelines.

The technical methods and techniques employed by the practitioner should be carried out within the remit of any associated published guidelines. The accompanying method is outlined in Chapter 5.2, The 2IR Methodology.

$TI_2^{(2)}$Ensure tools used are clearly understood and can be used by another investigator to produce the same results.

Practitioners must be technically capable of handling the tools chosen. They should be able to identify any issues with a tool and know the appropriate actions to take. Their use of the tools should be accurate and if used by another practitioner with the same devices/data, produce the same results.

4.1.4.4 Investigation Phase – Legal

The principles outlined here are standards to be observed that are specific to the Investigation phase but fall in the legal realm of the framework. This serves to inform and guide practitioners re the legal issues specific to this phase of the framework.

$LI_2^{(1)}$Ensure that methods used can be reproduced by other investigators producing the same results.

The methods used in a digital forensics process are integral to the legal acceptance of the evidence produced.

One of the main satisfying criteria for legal evidence that is produced from forensics is that of being reproducible. Practitioners must ensure that their methods are valid and recognized by others in the field. They should ensure that if the methods are used by another practitioner on the same data set the results should be similar. Technical methods employed widely throughout the Digital Forensics field include cryptographic hashes such as MD5 (message Digest Algorithm) and SHA1(Secure Hash Algorithm) variations. Procedural methods include creating and maintaining a chain of custody. Practitioners must ensure that their methods are reproducible with the same results. The methods used must be accepted by the community as satisfactory.

$LI_2^{(2)}$ Be aware of the laws associated with the investigation at this stage.

Laws are integral to any investigation and the practitioner must ensure that he/she is familiar specifically with the laws applicable to this phase of the investigation. The investigative phase is where the evidence for the investigation is gathered. Evidence is governed not only by laws of a state/country but also by principles and policies within an organization. A practitioner in forensics must ensure that he/she is familiar with all legislations within, and outside the organization.

Laws and policies relating to:

- General Laws regarding evidence(Rules of evidence)
- Gathering/ Acquisition of evidence
- Use of tools to gather evidence
- Environment is which evidence is collected and stored
- Digital evidence
- Electronic Discovery

4.1.4.5 Investigation Phase – Education

The principles outlined here are standards to be observed that are specific to the Investigation phase but fall within the education realm of the framework. They propose to inform practitioners of the basic education required to carry out this phase.

$EI_2^{(1)}$Ensure that the practitioner is trained to use at least three tools available whether open source or commercial.

Practitioners should be trained to use the tools available to them. Education and training are especially important at this phase, more so if the case should end up in court. Practitioners must be able to convince the court that they are appropriately trained to carry out the functions they purport to be experts in. This framework recommends that practitioners be formally trained to use at least two commercial tools and be experienced in manipulating a number of open sourced ones. Use of more than one tool in a digital forensics investigation helps to maintain accuracy of the results obtained. This practice helps to prevent and explain any discrepancies that may arise from the investigation (Ref. Casey Anthony Case – Section 2.3.3).

$EI_2^{(2)}$Ensure knowledge of the different tools to be used for different purposes throughout the examination. They should also be knowledgeable of the tools they work with and how they approach their work. Practitioners should ensure that they have received comprehensive training and practice in the tools that they will be using in any investigation. There are a myriad of digital forensics tools available and different companies and organizations in different jurisdictions use different tools. It is integral that when working as a team that decisive action be taken on the tools to be used by the group. All practitioners on the team should be trained to use the particular tools to be employed in-house. This is to ensure that practitioners have extensive knowledge and experience of using the specific tools as directed by the firm.

Below are some examples of software tools available. **NB** this is just a sample set of existing tools and by no means an exhaustive list. Additionally they are not the recommended tools that accompany the framework. Recommended tools are provided in the methodology section.

$EI_2^{(3)}$Treat all data and devices as potential legal evidence.

Throughout the investigative phase is where all the evidence is gathered. For this reason all data that is gathered throughout as well as any device that was picked up at the scene should be documented and a chain of custody maintained. This helps with keeping and ensuring that evidence gathered from all data and devices will be able to stand up in court. Practitioners should ensure that careful care is taken throughout the forensics process as at any time the devices being worked with and/or the data captured could be required as evidence in a court of law. Further specific guidelines are provided in Section 5.2 The 2IR Methodology.

4.1.4.6 Investigation Phase – Ethics

The principles outlined here are standards to be observed that are specific to the Investigation phase but which fall within the ethical realm of the framework. They serve as a guide to practitioners with respect to the ethical expectations of personnel in the field.

$E_1I_2^{(1)}$Maintain objectivity throughout the investigation

It is important that the practitioner maintain objectivity throughout an investigation. The practitioner should not allow any outside influences to affect the investigative process. All investigations are to be treated separately and should not affect the other. Objectivity is integral as all practitioners are expected to be unbiased in their explanation of findings resulting from the investigation. Careful adherence of the guidelines outlined in the 2IR Methodology in Section 5.2 helps the practitioner to remain objective throughout the entire digital forensics process.

$E_1I_2^{(2)}$Treat all data and devices as potential legal evidence. ($EI_2^{(3)}$)

Throughout the investigative phase is where all the evidence is gathered. For this reason all data that is gathered throughout as well as any device that was picked up at the scene should be documented and a chain of custody maintained. This helps with keeping and ensuring that evidence gathered from all data and devices will be able to stand up in court. The term forensics generally means for use in a court of law and thus even if the request suggests a routine process to establish who did what, when and by whom. The practitioner should at all times approach the digital forensic process with legal considerations in mind. Care must be taken with documenting all devices encountered and data retrieved to ensure adequate maintenance of a chain of custody and a defensible audit trail. This research presents a set of steps that ensures maintenance of a chain of custody. Additionally sample forms to be used by practitioners to assist are presented in the appendix.

$E_1I_2^{(3)}$ Exercise care to ensure the integrity of the evidence acquired.

Ensure validity and reliability in the materials analyzed; there are several ways to do this including maintaining a well documented chain of custody. Complete care should be taken to ensure that everything possible is done to maintain this chain of custody especially if litigation will take place. The 2IR methodology presented in this research ensures legal adherence including maintenance of a chain of custody. Example forms for the maintenance a chain of custody is outlined in Section 5.2, the 2IR methodology and forms to do so in the appendix.

Summary

This section presented Standards as the related directly to the Investigation phase of the digital forensics process. These standards are arranged based on the facet to which they are applicable. The policies presented outline that which must be observed specifically throughout the investigative phase. Those under the technical facet dictate those policies that pertain to the processes and the tools involved in the investigative phase while those principles listed under the legal facets looks at the procedures and laws involved at this phase. The principles listed under the educational facet addresses understanding and knowledge while those listed under the ethical facet address transparency and communication at throughout the investigative phase.

Reporting Phase – Technical

The principles outlined here are standards to be observed that are specific to the Reporting phase but fall within the technical realm of the framework. These serve to guide practitioners with respect to the minimum technical expectations during the reporting phase.

TR[1] Archive all software tools used.

Archiving assists with maintenance of the chain of custody. This involves the storing of all software tools used in the order in which they were used. This also should be dated and signed off. Keeping accurate records of the software tools used to acquire the evidence is especially critical if the case ends up in court and one is required to be an expert witness. It is important to note that not all cases go to court immediately. At times cases that originally started out as a routine check are afterwards involved in litigation. As an expert witness an investigator is expected to know details of the software used at different points in the digital forensics process and justify their choice and use of the particular software. Having this information carefully archived can prove especially useful if the case does not end up in court immediately as it can be easily retrieved. The specific steps outlining the archiving of software tools used are set out in Section 5.2, The 2IR methodology with sample documents are presented in the appendix.

TR[2] Archive all hardware tools used

Archiving assists with maintenance of the chain of custody. This involves the storing/recording of all hardware tools used at all stages of the process in the order in which they were used. This also should be dated and signed off. Different devices may require different hardware tools at different stages of the investigation. Practitioners need to record throughout the investigation the tools used. He/She will follow this up with archiving the information towards the end of the digital forensics process.

4.1.5 Reporting Phase – Legal

The principles outlined here are standards to be observed that are specific to the Reporting phase but fall within the legal realm of the framework. They serve to guide the practitioner as the legal requirements that must be observed at this stage of the digital forensics process.

LR[1] Document all hardware tools used in accordance with the recommended guidelines.

All hardware tools used throughout the investigation should be recorded and documented as per recommended guidelines and forms (Appendix B). This process also helps with the preservation of the chain of custody by showing what tools were used when and by whom.

LR^2 Document all software tools in accordance with the recommended guidelines

All software tools used throughout the investigation should be recorded and documented as per recommended guidelines and forms (Appendix B). This process also helps with the preservation of the chain of custody by showing what software were used when and by whom. This includes all software tools whether open source or commercial, this also helps in tracking and providing additional information that may be needed in the case of being an expert witness.

LR3 Regardless of legal definitions, a digital forensics practitioner will realize that there are degrees of certainty represented under the single term of expert opinion.

The practitioner will not take advantage of this general privilege to assign greater significance to an interpretation than is justified by the available data. The practitioner must act in fairness and without bias at all times.

4.1.5.1 Reporting Phase – Education

The principles outlined here are standards to be observed that are specific to the Reporting phase but fall in the education realm of the framework. They serve to guide practitioners and outline the basic knowledge required during this phase of the digital forensics process.

ER^1 Practitioners must be knowledgeable in the archiving and documenting tools used

Practitioners must possess the knowledge base to correctly document all the tools used according to the stipulated guidelines [See appendix A]. Following this these should be archived for easy and timely retrieval.

ER^2 Practitioners must be adequately trained to produce a comprehensive report of the investigation.

A comprehensive report of all findings resulting from the investigation must be created and disseminated to all stakeholders. This document must be free from industry specific jargon and simple enough to be understood by most readers or listeners. This is not aimed to take away from the uniqueness of the field but help in comprehensibility. The comprehensive education programme presented in this research addresses the need for adequately trained digital forensics practitioners. A sample comprehensive report form is presented in the appendix.

ER^3 Possess enough training to interpret findings accurately, apply them to creating a relevant attacker profile and reconstructing the digital incident scene.

The main objective of any forensics process is to identify who did what and when and thus any training in the field should reflect this. Included in any digital forensic training should be a section on creating an attacker profile and reconstructing the digital incident scene. Practitioners in the field should have enough education background to do this in an attempt to identify or present a suspect of any unauthorized access case as a result of correct interpretation of findings. Reconstruction of the scene of the incident is critical to solving any issues with regard to why the request was made initially. Practitioners in the field of digital forensics should ensure that they are educated in all the required areas including reconstructing the incident scene. In recognition of the need for such trained professionals in the field this research presents a curriculum of studies that includes reconstruction of the crime scene which should be an integral part of any course or curriculum designed to address digital forensics as well as the reconstruction of an incident scene.

4.1.5.2 Reporting phase – Ethics

The principles outlined here are standards to be observed that are specific to the Reporting phase but fall within the ethical realm of the framework. They serve to guide practitioners as to their ethical expectations during this phase of the digital forensics process.

$E_1R^{(1)}$ Practitioners must ensure confidentiality in the findings of the investigation.

As a practitioner the importance of confidentiality throughout and at the end of an investigation cannot be over estimated. All findings from any investigation, after being carefully documented and a report produced, should be disseminated only to the relevant stakeholders. Whatever the type of case this confidentiality should be maintained and the practitioner should not disseminate information pertinent to the case via any form of public media without communication with, and gaining permission from, the immediate stakeholders.

$E_1R^{(2)}$ Practitioners must ensure full disclosure of their findings to the relevant personnel.

When a practitioner works as an expert witness they will not take advantage of the privilege to express opinions by offering opinions on matters within their field that is not necessarily their area of expertise. Practitioners should ensure that their full findings are disclosed only to personnel involved with the case.

Conclusions should not be drawn from materials that are atypical and/or unreliable (cannot be validated or verified) or that the practitioner is unsure of. Where results are inconclusive or indefinite any conclusions drawn should be fully explained in the report with supporting facts. Content should not be added or removed from the findings for sensational purposes on the part of the practitioner for personal gain.

The standards/principles outlined in this section are specific to both the phase indicated as well as the facet as shown. They are designed to encompass the basic operating parameters for a practitioner in the digital forensics field. Here the standards/principles are presented under the appropriate headings accompanied by an explanation of the standard. These standards should not be interpreted as a separate standard in its own right but as part of the overall structure, the framework.

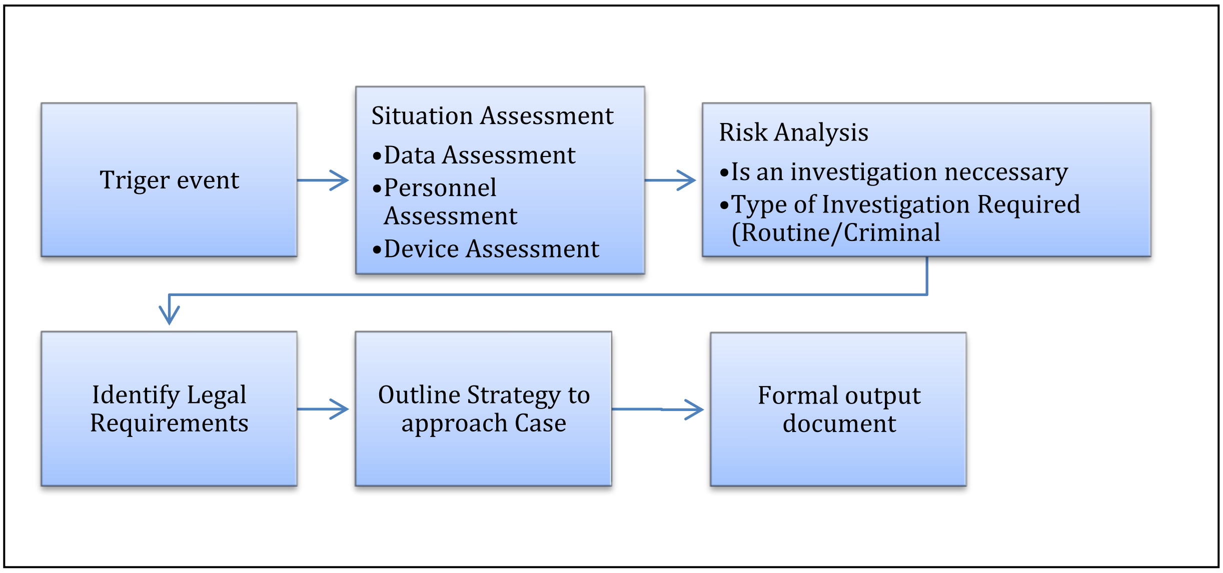
The standards outlined are designed to provide a basic framework within which all digital forensic practitioners should operate from the initial point of entry into the field. Appropriate self evaluation, reflection, ethics and professional development are all critical elements to improving a practitioners practice as well as the field as whole. These standards indicate key areas which a practitioner at all career stages should observe.

4.2 The 2IR Methodology

The 2IR Methodology consists of three distinct phases. These phases, specifically the second phase, consist of tasks that are common to other methodologies such as (Yong Dal 2008) (Perumal 2009) (Kruse and Hieser 2001)) (King 2006). The 2IR methodology differs in that it groups these activities under one phase, the investigation phase. This is in order to show that the digital forensic process begins at alert, the actual investigation begins on arrival at the incident scene after collecting preliminary data. Other existing methodologies/models equate the entire digital forensics process to the activities presented as the investigative phase (phase 2) Another uniqueness of the 2IR methodology is that it includes the recommendations of the use of at least two different tools in the copying, preservation and analysis of digital evidence. Some commercial tools come with their own instructions which may be deemed as a methodology. There are also methodologies that have been developed by practitioners such as Brian Carrier who has also developed several tools including Autopsy Forensics Browser. However the 2IR methodology has been developed independent of any tool but makes recommendations based on criteria highlighted in Section 5.2.1. The 2IR methodology also includes both the creation of an attacker profile and recreation of the incident scene together before conclusion of the process. While there have been models created with the inclusion of a reconstruction of the crime scene and/or creation of an attacker profile this methodology (2IR) includes them both with other steps not combined before in any other methodology. The methodology draws on aspects of the Electronic Discovery Reference model for electronic discovery, e-discovery being an integral part of cyber/computer related investigations retrieving electronically stored data.

Another novelty of the 2IR Methodology is that it includes a formal output document at the end of the phase aside from the formal report required at the end of the digital forensics process. Also included in this methodology is the highlighting of the need for continuous status reporting throughout the entire digital forensics process and production of a defensive audit trail.

4.2.1The Initiation Phase (I)


Triger event
Situation Assessment
•Data Assessment
•Personnel Assessment
•Device Assessment
Risk Analysis
•Is an investigation neccessary
•Type of Investigation Required (Routine/Criminal
Identify Legal Requirements
Outline Strategy to approach Case
Formal output document

4.2.1 The initiation phase

The initiation phase consists of some tasks referred to and/or grouped in other methodologies such as preparation (Yong Dal 2008) and as alert by (Perumal 2009).

The aim of the initiation phase is to set the stage for the production of digital evidence that will be admissible in a court of law. All requests involving electronically stored information should be approached with litigation in mind. This section outlines the tasks that are critical in ensuring that the necessary actions are carried out and appropriate documents requested and produced before any device is accessed or seized. This stage assists in determining if there is actually a case to be investigated and if there is a case how it will be approached. The initiation phase promotes careful assessment and planning. It consists of several tasks to be completed before the output document can be completed. A documentation of all the facts related to the incident must be completed in order to assist in preserving the chain of custody should the case end up in court.

The actual process for a digital forensics investigation unlike e discovery begins at the request for such services. (Hewling 2010) asserts that this is the trigger for the investigation. The moment this trigger event occurs the person in charge assigns a member of the digital forensics team to do an assessment of the situation.

4.2.1.1 Assessment

The assessment will provide the information regarding the scope and intent of the investigation as requested by a client. A general situation assessment is to be undertaken and can be categorized as personnel, data and device. These are integral components of the investigation and the practitioner needs to be aware of their status. These include, Personnel Assessment, Data Assessment and Device Assessment

- Personnel Assessment

An assessment of any personnel connected or possibly connected to the incident should be completed. Immediate personnel involved (if known), connected or aware of the incident could provide information relevant to the conduct of the investigation. They need to be assessed so that the practitioner is able to ascertain how much information they are able to contribute to the investigation proving relevant leads that would influence the direction the investigation should/could take. It should be ascertained by the practitioner whether it is known to the requester how many persons are suspected to be involved. This of course is dependent on if it is known where the intrusion originated. When dealing with an organization the practitioner will need to ascertain if the source of the intrusion was internal or external. If it is external then the practitioner will want to consider interviewing to find out who could have any possible motive. If the intrusion has an internal origin then personnel assessment becomes simpler as that would suggest that it is likely that the perpetrator is from within the company or has access to someone or facilities within the organization. The practitioner needs to find out if there are any personnel who have specific knowledge of the incident. Is there and internal team assigned to the incident. The Electronic Discovery Reference Model also suggest that the practitioner ascertains if there is any special access granted to key personnel. It is at this point that the practitioner will need find out who will be the point of contact and whether or not he/she will be working with anyone else on the investigation.

- Data Assessment

An initial data assessment will assist in estimating the amount of data that the practitioner will be working with. This assessment will also help to determine the type of data being dealt with and where data relevant to the case is likely to be found. Data assessment will help to identify key data sources and what type of data may be encrypted and password protected. Questions such as: where is the bulk of the data in case of an organization is stored? Is there a particular document management system? And is data stored in a central spot such as file server or on local dives or both? If there are servers in use where can they be found? In the case of an individual it should also be ascertained what email and/or cloud services are used. These questions are all relevant and pertinent in that they help to determine the flow of the investigation, influencing other factors such as the skill that will be required for the investigation, as well as the devices/tools that will be needed. Additionally having the access to data stored on third party systems (eg. email and cloud storage)whether the client is an individual or an organization will have a significant effect on planning The practitioner/investigator will need to know the different firms with which to make contact with regard to accessing data relevant to the investigation.

- Device assessment

A general assessment of all devices involved in the intrusion will help to determine the tools to be used throughout the process. It will also help to establish how quickly an action is needed from the digital forensics team. From this exercise it should become clear what the types and estimated number of devices involved are. It should be identified whether or not special tools are needed to collect particular types of evidence. In the case of a large organization with fully networked systems (Casey 2004) suggest that the practitioner ascertains if the systems can be taken offline for the collection of data. Information is also needed to find out if the data on these devices are backed up centrally or in particular areas. In the case of an individual it is important to find out who owns the device and can it be taken away for examination. In a criminal case these become less of a challenge as law enforcement may be able to dictate such actions.

4.2.1.2 Risk Analysis

It is during the initiation phase that the practitioner will do a risk analysis to determine whether or not the case is feasible. During this phase the personnel involved in the case will identify particular issues relevant to the case that may make it vulnerable and weigh its impact. The practitioner needs to, at this point, determine the limits of their authority and ensure that all boundaries are made clear. General risk related questions that need to be answered include:

- What are the expectations of the stakeholders? Why was a forensics investigation requested and what is it that they expect of the process/ What type of investigation is to take place, is it in response to a criminal issue or is it just a routine check?
    - What is the intensity of the situation?
    - What type of intrusion occurred (if any), internal or external?
    - Does the case require immediate attention or can it be delayed?
    - Who know about the call for a digital forensics practitioner?
    - Is it possible that evidence can be destroyed before the process begins?
    - Is the suspect known and if so what are their technical capabilities, what is their level of security access. Is it possible that there are others involved?
    - If the suspect is unknown what is the possibility of inside assistance?
    - Is the situation time sensitive – what time frames are involved?
- Is there any other type of evidence other that resides in the digital realm?
- How valuable is the evidence to be recovered?
- Are there any budgetary constraints?
- Who will provide the needed resources for the digital forensics process and how will additional resources be sourced?

a. Personal Risk analysis

If the practitioner is working as an individual there a particular question that should be asked;

- Are the tools necessary for use in this particular investigation available?
- Are the requisite skills required for this investigation available?
- What are the costs involved and can it be fully funded?
- Can the process be completed in the time frame allotted by the client?
- Is there any part of the process that may be outsourced and if so will the client be comfortable with such an arrangement?
- Does the practitioner and/or team posses the required qualification to be an expert witness if required.

b. Company risk analysis

There some issues that may directly impact on the productivity of the company and this risk must also be assessed.

- How much downtime can the organization afford (if any)?
- Is the company willing to risk the exposure that may result from the investigation?
- Is the company willing and able to spend the monies to be incurred throughout the investigation?
- Will this be value added for the organization or will it result in a loss?
- How will the investigation benefit the company if at all?

4.2.1.3 Legal requirements

The legal requirements for the digital forensics process must be identified (King 2006). It is important to determine the type of investigation that will be conducted. It should be made clear whether the objective is to bring a criminal or civil case or otherwise. All restrictions pertaining to the process must be identified. This will help to ascertain if the organization (or requester) has particular policies and regulations in place with respect to information security, digital investigations and electronically stored data. It is highly recommended that the practitioner ensures that contact is made with the lawyer/legal advisor of the client. It is also important to clarify any restrictions, constraints and additional legal issues regarding the request to ensure a defensible audit trail.

The digital forensics providers should endeavor to identify all possible sources of data and request authorization to cover all these sources. (Chisholm 2010) notes that "when requesting authorization to search and seize the practitioner/s must ensure it covers all equipment to be included in the investigation". This is essential because only equipment covered by the authorization can be included in the process. While authorization can be amended at a later date the situation should be avoided as much as possible. The can be achieved by having a carefully prepared plan in place.

The digital forensics teams must document any particular escalation procedures the company/client may have in place. Take note of who should be notified of any issues related to the process. Knowledge of the intent/objective of the digital forensics request cannot be over emphasized though despite this chain of custody must be preserved to ensure a defensible audit trail.

- Case Strategy

A plan should be developed outlining the overall strategy to be employed throughout the case. This plan should be repeatable producing similar results if used by another. This plan is the beginning of a defensible audit trail. It does not have to be elaborate but will help to ensure that all bases are covered. The approach and strategy used will vary depending on the requesting party. Whereas procedures in dealing with private organizations as opposed to law enforcement or individual requesters may vary, the base rules of chain of custody will apply whoever the client may be. Laws such as those addressing privacy, misuse of computers and evidence must be held in high regard. Having a plan however miniscule will enhance the quality of the digital/electronic evidence while lowering the risk factors and potential to the case and/or investigation.

- The plan

The plan will outline the tasks, tools and general resources to employed throughout the process to recover, analyze and present the digital evidence found. This plan will in addition to ensuring that all bases are covered, help with the managing of the process and to an extent budgeting. Items to be covered by the plan include, chosen team, keywords to search, summary of major tasks, timeframe of the incident, investigation, key persons, reporting schedule, documentation format and validation methods. These elements are critical as they outline the base from which the practitioner will approach the investigation.

- Team
- Keyword list
- Summary of tasks
- Timeframe of the incident
- Timeframe for the investigation
- Key personnel
- Status reporting schedule
- Documentation
- Validation
- Team

The selection of suitably qualified and experienced personnel to handle the case is essential. Depending on the origin and type of case the team may vary not only in size but in terms of expertise required. There is the possibility that one practitioner may be able to handle an entire case whereas in other cases several practitioners may be required. If an investigator is working with law enforcement on a criminal case then the team structure will quite likely be decided by them. However if there is a forensics team contracted the team will have to be decided in-house based on expertise and experience. This may be based on preferred skills in the digital forensics field such as penetration testing, case management and/or mobile forensics.

- Keyword list

As the initiation phase proceeds particular jargons and acronyms used within the organization that may be relevant to the case should be identified. From this a list key words to aid with the data search is to be compiled. If the case is one required by an individual the keyword list can be created during interviews and or from information received about the case from elsewhere.

The main objective of the plan is to put in place a structure to guide the digital forensic process that is about to be carried out. It will help to justify the approach being taken to the investigation. This plan will include a summary of the pertinent information gathered from the fact finding process. This summary must include:

- All the types of data to be captured
- Key personnel related to the investigative process. This includes, witnesses, suspects and other stakeholders such as management.
- All potential data sources identified.
- Backup media, onsite and offsite
- Recovery systems, live and retired
- Servers
- Auxiliary media, mobiles, USB drives, tablets
- Third party storage, ISPs, cloud, public email servers
- VOIP storage, company intranet, IM storage
- Employees personal devices

These elements are important inclusions for a number of reasons including the fact that it is a good foundation for the preparation of the final report and includes critical aspects needed to guide the practitioner throughout the investigative phase.

Documentation is essential throughout the entire digital forensic process. This point is supported by practitioners such as (Casey 2004) (King 2006) and academics in the field such as (Carrier and Spafford 2006). Its importance cannot be over emphasized. Documentation is valuable from as early as this stage so that if and when particular questions arise the answers would have been recorded. It also demonstrates that at each stage records are maintained and thus more defensible. This documentation also helps to make up a case file and thus timely and accurate documentation of activities and findings are critical. Accurate documentation indicates the level of organization on the part of the digital forensics practitioner/team. It is important to ensure that the process used is repeatable and will produce similar results each time it is used.

NB. Suggestions

The following are some suggestions to ensure a defensible plan and resulting output document from the initiation phase are produced. This information could provide relevant and critical information that will assist in the digital forensics process. Refer to the 2IR framework (Section 5.1) for standards related to these important inclusions.

- Ensure consistency and eliminate exclusions by identifying clear objectives and expectation from the outset.
- Create a list of key personnel who can assist throughout the investigation.
- In the case of an organization, create a list of the various departments that may be potential sources of information relevant to the investigation, include all relevant information on witnesses and suspects and decide how their involvement with the case be handled.
- Note information on all systems both hardware and software and decide how they too will be handled. Will they removed to a controlled area or will they be imaged onsite. Information to gathered re the systems include;
    - Type of Operating System
    - Hardware platforms
    - Number of types of systems involved
    - Types of Systems (laptops, desktops etc)
    - Hard drive types if any and configuration, number of hard drives and their sizes
    - Locations served offsite vs onsite
    - Remote servers location and type

- ISPs and cloud service providers

- Make careful note of any timeframes stipulated by the client. It is important to ensure the time frame is realistic before starting a project/investigation. If working with law enforcement on a criminal case time may be critical.

- It is recommended that the practitioner should ascertain if there are systems that purge data at regular intervals and include in the plan measures to preserve data on these systems. If the system eliminates data at set intervals it could mean that relevant information can be deleted before the practitioner gets to the device and thus this needs to be known and planned for.

Collect all documentation relevant to the investigation such as

- Systems lists
- Development plans
- Any maps or diagrams
- Flow charts and data flow diagrams
- Schedules
- Organizational charts

It is important to ascertain if the client has undertaken any damage assessment before alerting a practitioner. Make note of this in the plan.

From the fact finding session there should be a list of the evidence (devices) that will need to be processed. Ensure inclusion of remote sites used for storage, backup and hosting.

Unless it is a criminal emergency situation, and even then there should be time line for the investigation, which is updated regularly.

- If the practitioner works independently ensure there is a skill set possessed to cover all the requirements of the investigation. Outsourcing may be considered. If the project is to be undertaken by a team it should reflect the skill set required by the investigation.

Suggested Tools

These tools are recommended based on certain positives. They have components addressing all aspects of the digital forensics process. Their use and reliability in the field internationally makes them acceptable in most jurisdictions worldwide. Additionally the tools recommended posses the following characteristics:

1. Updated regularly - the recommended tools are regularly updated to accommodate changes, fixing of bugs and technological advances by the developers. This helps to ensure the receipt of more reliable and verifiable data.
2. Widely used across jurisdictions – these recommended tools are available and have been used across all jurisdictions by practitioners worldwide (See chapter 4)
3. The recommended tools have been deemed to be reliable as they are able to reproduce similar results despite the condition of use. Reliability in this context refers to the ability of the tool to perform its core functions whatever the circumstances and whoever the practitioner is.
4. Academic input – Research and development is integral to any field and the tools in use within that field. The recommended tools are from companies that have an active research and development arm that ensures that the tools are constantly updated and are relevant to the current technologies available.

The recommended tools to be used with the 2IR framework and methodology are based on the criteria listed above.

- Forensics toolkit (FTK) this is a tool created by Access Data one of the leading Digital Forensics companies. They create tools for Digital forensics, Cyberforensics and Ediscovery coving all the requirements of the 2IR methodology. Access Data, a US based company trains practitioners in the use of their tools and has six training centers worldwide as well as eight training partners who facilitate this training. They have also partnered with academic institutions worldwide to provide training and facilitate research and development and by extension improvement in their product.

- X-Ways Forensics

X ways is an integrated suite of digital forensic software developed by an online company X ways software technology AG. The company based in Germany produces software addressing both digital forensics and e discovery. In addition to the integrated software suite they also have software addressing different stages of the digital forensics process. X Ways also provides land based training in the use of the various digital forensics software they develop in countries worldwide. The software is available in six languages and is regularly updated to suit the needs of the dynamic technological industry.

- EnCase

Encase is developed by industry leaders Guidance Software. It is complete suite of digital forensics software that addresses both computer forensics and e discovery. This suite of software addresses different stages of the digital forensics process. Guidance Software also provides a training in using their software tools. Guidance software tools are widely accepted worldwide and thus are widely available.

Summary

The initialization phase of the 2IR methodology sets the stage for an investigation that will satisfy legal, ethical, educational and technical criteria. This phase may take the form of interviewing one or more stakeholders in the investigation ensuring the collection of all relevant data need to set the stage for a thorough investigation.   This stage is divided into a number of steps and seemingly involves getting a lot of information however it is time sensitive and must be completed in as little time as possible while maintaining accuracy. This should be done without compromising the integrity of the entire digital forensics process. (Chisholm 2010) notes that the main goal of the digital forensic process like e discovery is to “ensure that data collected and preserved is legally defensive and forensically sound”. Despite the time sensitive nature of the process careful care must be taken to preserve the chain of custody.

4.2.2 Investigation Phase {I}

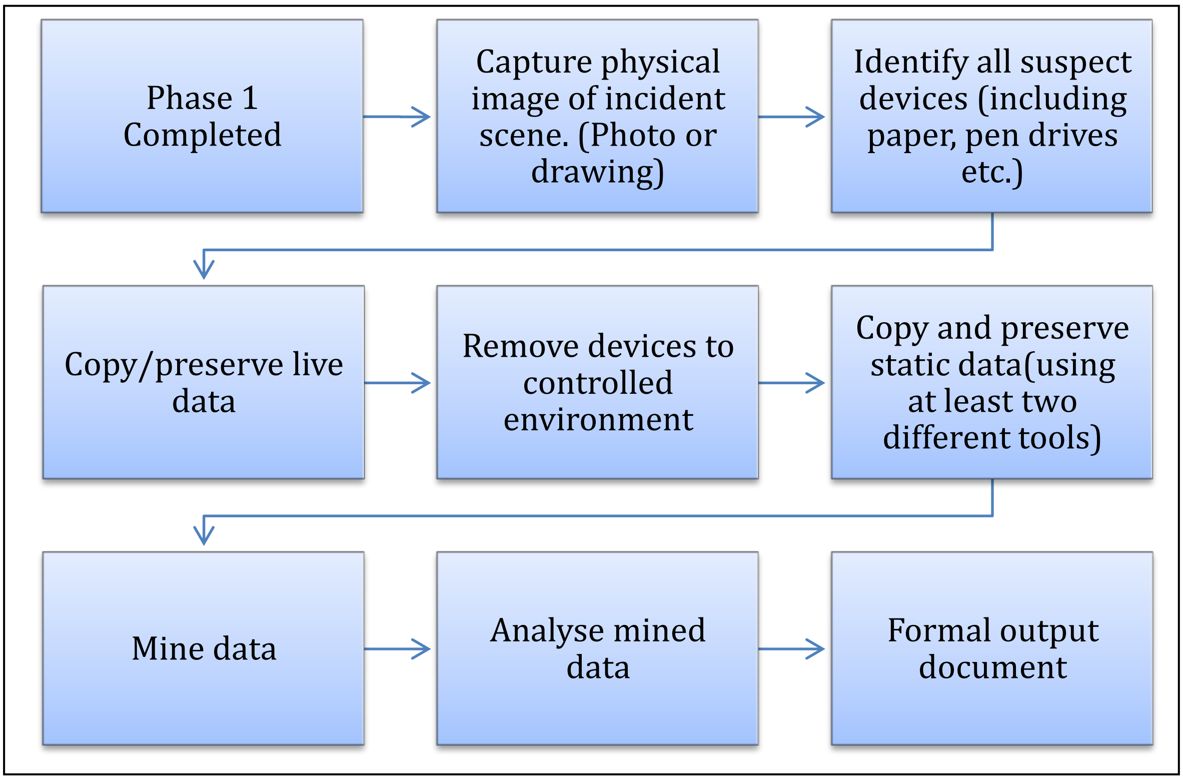

Phase 1 Completed
Capture physical image of incident scene. (Photo or drawing)
Identify all suspect devices (including paper, pen drives etc.)
Copy/preserve live data
Remove devices to controlled environment
Copy and preserve static data(using at least two different tools)
Mine data
Analyse mined data
Formal output document

Figure 5.8 Stages of the Investigative phase of the 2IR Methodology

Upon completion of the initiation phase with an investigation plan in place and proper authorization received, the practitioner can move onto the investigative phase provided a case had been established from the initial phase. The aim of this phase is to produce digital evidence that is valid and verifiable. This digital evidence should be reproducible and able to withstand the rigor of the legal environment. This is the most comprehensive phase of the 2IR methodology.

Phase 2 of the 2IR methodology is the bringing together of a number of activities involved in the digital forensics process. This is where definitive identification of the source of the information, preservation, collection, examination and analysis of digital evidence will take place. These are all activities included in the other methodologies developed such as (Casey 2004), (Hewling 2010), (Agarwal 2011) and (King 2006). The 2IR methodology however groups these tasks differently eliminating redundancies and presenting an integrated approach to the process.

If the investigation is being carried out in an organization by a team, each team member should be assigned a specific role. This role should be ideally related to their training and experience. Before commencing the investigative process ensure that there are adequate resources such as evidence forms and bags. Each time a new piece of evidence is discovered it should be treated with the same seriousness as the initial set collected. The first activity at this phase involves the activation of the preservation plan. This will include preserving and processing the scene of the incident.

a. Capture a physical image of the scene of the incident

Getting a physical image captured of the scene of the incident is integral to all forensics examinations (Casey 2004), (Carrier 2006). Having a copy of what the scene looked like when the practitioner first got there is an important part in the preservation of the chain of custody. This image is basically an image/diagram outlining what the situation at the scene was initially and can be captured using different methods preferably a digital camera. This point is supported by (King 2006) stating that the incident scene should be photographed. It is important to note that the incident scene includes notes, loose paper, filing cabinets, desk and contents, drawers, books and cables. This is done not only to preserve chain of custody but critical information could have been written and hidden in various areas on or close to the scene that may prove useful to the investigative process. In the case where the investigation is taking place within an organization and computers connected in a network, a request for the network diagram showing the layout and location of all devices should be made.

b. Identify suspect devices

The incident scene should be processed with collecting physical as well as digital evidence. This phase can prove to be more complicated than the others with the type of physical evidence that will need to be addressed before moving on to the digital realm. All physical evidence related to the incident including documents as well as auxiliary storage media, hard copy documents and note papers should be identified and recorded. (Hewling 2010) highlights some key points to consider on arrival at an incident scene. These include:-

1. Identify all hardware devices additional to the suspect device within close proximity of the incident scene (mobile phones, laptops, tablets, printers). Careful note to be taken of USB drives in particular as they are easily disguised and the practitioner must be thorough.

2. Look for disks/auxiliary storage that may contain programmes/software proving useful to the investigation. For example if the incident involves accounting data, a particular accounting software may prove valuable to the practitioner.

3. Take careful note of any bits of paper such as “post its” that may contain information proving valuable such as PINs, log in information, passwords etc. Look out for such in places such as bins, under keyboards, side of desks etc.

A key point to note is that if at this point the suspect device/devices are on with systems running the practitioner should check the system clock against current time along with the programmes running saving the contents of open applications. The objective of doing live forensics is to ascertain what is happening just now, who is doing what on the system/s (Adelstein 2006). Due to the nature of digital crime scenes there may be need to process some devices on spot while others may be transferred to a controlled environment. “Volatile evidence should be should be processed as quickly and as efficient as possible” (King 2006). After identifying suspect devices and capturing a physical image of the scene volatile data should be captured. Memory dumps, network connections etc should be captured as quickly as possible.

There is the possibility that there may be times when a practitioner may not be allowed to remove the suspect devices to a controlled area and thus imaging of the device would be done at the scene. While it is best to image a device such as a computer while it’s not in operation the requesting party may stipulate this. There will be times when the case is not initially criminally motivated. If this is deemed to be a routine or suspect check by an organization, careful care must be taken by the practitioner to observe the surroundings of the incident for loose items that may prove integral to the case should it end up in court and thus all digital forensics investigations should be approached keeping this in mind.

After copying and preserving volatile data the practitioner will seek to remove suspect device/s to a controlled environment. Seizure of devices essentially taking place at this point. Whereas circumstances may differ with regards to evidence required, incident, type of investigation and even the investigator it is recommended that the suspect device be removed to a controlled area. (Hewling 2010) asserts, “The device being investigated due to the sensitive nature of digital evidence, should be removed from the incident scene to a controlled environment where it can be thoroughly examined”. (Carrier 2002) also support this point noting that it is important to remove the suspect device from the scene of the crime to a controlled environment for examination.

On seizing computer hardware an unformatted floppy may be placed in any floppy drive or equivalent present to prevent accidental booting or rebooting of the system. There are organizations that install utilities to erase files at start up and shut down thus the practitioners need to ensure that measures are put in place to prevent accidental erasure of evidence. The use of hardware digital forensics tools as recommended in the tools section should be used. It is also recommended that the device be disconnected directly from the power source (Hewling 2012) (King 2006) (Casey 2004) and evidence tapes be placed over plugs and subsequently signed and dated by the practitioner. This also helps in maintaining the chain of custody. All seized devices should be packaged, sealed and labeled and stored in a secure area and protected from electromagnetic radiations, dust heat and moisture.

Following the collection and preservation and seizure of devices they (the devices) are then moved to a controlled environment. This environment should already be equipped with the necessary tools and trained expertise to carry out the duties required. Having had an evidence collection plan in place the practitioner will ensure that all evidence collected is recorded. This record should correspond with the previous document containing the information on what evidence is to be collected, assuring integrity of the evidence and accountability on the part of the practitioner.

c. Controlled environment

It is recommended that all evidence collected be reviewed and analyzed for data relevant to the case for leads, (King 2006) supports this point noting, “Leads can come from reference documents, notes on sticky pads, desk blotters, printed emails, desk calendars, book marks, photographs, business cards and many other forms of physical evidence”. Keeping this mind the practitioner should ensure that all potential evidence in the vicinity is checked and recorded for relevant data and information. In the controlled environment for example forensics lab all media to be used should be verified and useable before the digital forensics process begins. This is to ensure the prevention of data corruption from previous activity. All digital media should be properly sanitized after each use to prevent the transfer of data from previous investigations to current data being investigated. .

Before the investigation begins a bit stream copy of the disks to be analyzed must be taken to ensure the original remains intact. (Hewling 2010) supports this point by recommending that an image of the disk to be investigated be captured and actual work be done on the original disk. This is further supported by (King 2006) "Analysis, research or any investigative work must never be performed on the actual digital evidence or forensics image". He continues "it is highly recommended that at this point "a working image" of the device be taken". The point is reinforced further by (Schatz 2007) "Process forensics image working copy only". It must be noted that different methods of copying the evidence should be used. No single method guarantees retrieval of all data thus using more than one is recommended to ensure reliability.

Having created a working copy the investigator now moves on to mine and analyze data. The practitioner will then:

- Extract all allocated data from the partition/disk to be processed.
- Carefully check the slack/free space for any data that may be there.

(Hewling 2010) notes that "hidden data as well as previously deleted data will reside in this area and thus they must be carefully examined for such". (King 2006) indicates … "as files are deleted or over written, remnants of previous files using the same physical area on the disks may exist". The remnants of data found in theses spaces may prove to be useful evidence when checked and analyzed by the practitioner.

- Carefully scrutinize swap space as it too may also contain valuable data relevant to the case and thus should be carefully checked.
- In the case of windows based computers it is recommended that the following be checked for relevant data.
    - The page file system (also referred to as the windows swap file)
    - The hiberfil.sys. This is the file used when a computer goes into hibernation. Process information and the contents of memory are written here and thus should be searched for potential fragments of information.
    - The Memory dumps should also be checked.– If a live system is being imaged it could contain valid information such as user ids and passwords, websites visited, documents and images that were running at the time of the capture. Memory dumps are especially useful when doing network forensics.

Having collected the evidence the practitioner proceeds to refining the evidence collected. The practitioner then continues to carry out the following as adapted from (King 2006) and (Casey 2004):

a. Identify and process the composite files

b. Identify and process any encrypted password protected files

c. Identify and process the email repository and attachments

After completing the identification and processing of composite files, encrypted and password protected files along with the email repository attachments the practitioner moves on to data reduction. “Data reduction is the process in which the amount of data or quality of files to be analyzed and processes are reduced” (King 2006). The investigator then continues to generate file lists and hash values.

The practitioner then moves on to the processing of the refining evidence. This process includes the following steps:

1. Categorizing the files using a commercial tool such as the “sorter” programme that comes with the sleuth kit package. (Sleuth Kit is one of the recommended tools)

2. The comparing of file extensions to actual file contents.

3 The documenting of any hidden data recovered.

4 The documenting of any investigative leads uncovered.

5. The investigator then searches the accumulated data for keywords, keyword phrases, text strings, names and other specific information to find files that contain particular references. The more specific the search the more likely that it is that the search will produce investigative leads.

6. Review all file contents and refine all findings.

d. Analysis

This is the most critical stage of the investigation and dependent on the practitioner’s expertise and experience as it is open to interpretation. There are at least three levels involved in analyzing digital evidence which may be categorized as temporal, relational and functional (King 2006):

a. Temporal analysis

Temporal analysis is an important factor in the analysis of digital evidence and can prove very critical in the reconstruction of sequence of events in the incident. Temporal analysis is the process of correlating known occurring events with digital object dates and timestamps

b. Relational Analysis

Relational analysis involves establishing relationships between the digital objects and other aspects of the investigative process. In doing this the practitioner will endeavour to show how the various components connect, how different pieces of evidence correlate.

c. Functional Analysis

Functional analysis establishes the dependency of functions and objects in the investigation on each other. The greater the reliance the more the objects are deemed to be connected.

Summary

The investigative phase of the digital forensics process is the most complex of all the phases relative to any methodology used, Sections of the Investigative phase were adapted from the work of (King 2006), (Hewling 2010), (Chisholm 2010) and the E-Discovery Reference Model Each of the sections in the above methodology are compiled to ensure accurate identification, collection and analysis of evidence, identification and mitigation of limitations as well as proper management and analysis of the data collected/found. The digital forensic investigation is more uniformly completed with the aid of a properly prepared plan as recommended in the initiation phase serving as a guide throughout and containing information and data that will prove useful throughout the investigation. Random collection and processing of evidence can present problems in the latter stages of the investigation such as a poorly created chain of custody. Additionally it is deemed unprofessional and leaves one open to external unfavorable criticisms. This is supported by (King 2006) “A forensics plan ill conceived or poorly executed will result in enormous waste of resources and evidence”. The use of plan ensures proper documentation and should evolve as the investigation progresses.

4.2.3 Reporting Phase {R}

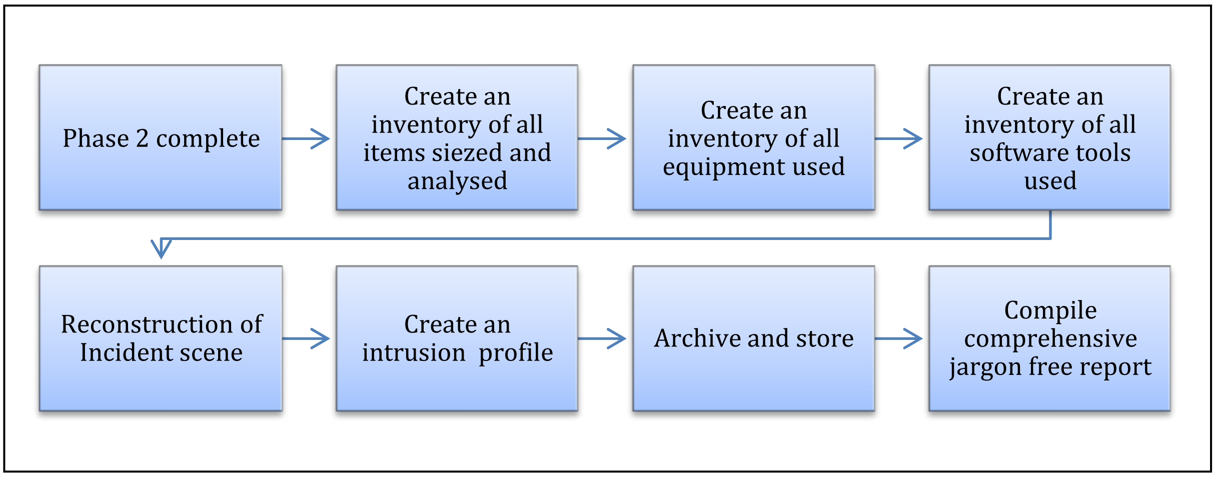

Phase 2 complete
Create an inventory of all items siezed and analysed
Create an inventory of all equipment used
Create an inventory of all software tools used
Reconstruction of Incident scene
Create an intrusion profile
Archive and store
Compile comprehensive jargon free report

Figure 4.9 Stages of the Reporting phase of the 2IR methodology

The reporting phase is the representation of a culmination of all activities. It is important more so because this is where all the data gathered and analyzed comes together and is prepared for further action. This stage is referred to as 'presentation' in other methodologies (King 2006),(Agarwal 2011) (Ren and Jin 2006) while (Selamat 2008) refers to this stage as presentation and reporting with an additional phase referred to as disseminating the case which are all included in the reporting phase of the 2IR methodology.

This phase begins following the extracting and analyzing of the evidence collected. The practitioner now proceeds to organizing the information received including evidence logs, witness statements (if any) along with digital evidence analyzed. All this must be collected and collated. The first step of the reporting phase is to create an inventory of all items seized by the practitioner for investigation.

This then followed by the creation of an inventory for all equipment used throughout the investigation. There also needs to be an inventory of all software tools used during the different stages of the investigation.

Also included in this phase is the reconstruction of the event scene and the creation of an attacker profile. These two sections are unique to the 2IR methodology. Whereas they have been included in other methodologies by themselves (Lee 2001) (Shin 2008), the research did not find any that incorporated both these actions together during this phase.

a. Reconstruction of the event

The main objective of the digital forensic process is to identify what happened, when it happened and who did it. Reconstructing the incident scene from the data gathered is helpful in this regard. Reconstruction of the incident scene helps to establish what happened and when and possibly by whom. This process is needed to help with nullifying any vagueness in the analysis of the digital evidence. It reduces any erroneous conclusions thus making the data analyzed more reliable. Event reconstruction helps to reinforce the techniques and methods used making them more transparent and thus increasing evidence admissibility.

Reconstructing the incident scene is done by investigations regularly to narrow the perpetrators of a crime. In digital forensics there are a few emerging theories re its use in the field (Hargreaves and Patterson 2012) (Rogers 2003). An issue of Digital Forensics as presented by Hargreaves and Patterson is that the field faces the challenge of having a large amount of data to work with. These large amounts of data resulting from the capacity of the devices being worked with as well as the number of devices that may be involved in the case. This challenge however should not serve as a deterrent as the ultimate goal of any investigation including a digital forensics investigation is to identify (or come as close as possible to) the person responsible for an incident. Temporal Analysis is very important when presenting the reconstruction of the incident scene as it is what correlates the known events with the digital object dates and time stamps.

b. Creating an attacker/offender profile

Criminal/offender/intruder profiling is categorized as either inductive or deductive. Inductive suggesting general to specific, looking at general behavior patterns from criminal databases of previous offenders and narrowing it down based on certain predetermined criteria. Deductive however looks from specific to general (Turvey 1999). The focus is on the particular case being dealt with. Looking at the evidence from the particular case to construct behavioral patterns specific to that case. Both methods though widely used are not usually able to specifically identify the person responsible but has proven valuable in reducing the number of specifics in a case. (Douglas et al 1998). Creation of the offender profile however allows the practitioner to reduce the number of suspects making it easier to trace and identify the perpetrator of the incident.

The practitioner or forensics team will then archive and store all items used during the investigation before creating a comprehensive report of all procedures and findings.

Summary

The reporting phase of the digital forensics process is critical as it is where all the information gathered comes together in an effort to pin-point what happened where, when and by whom. During this phase the practitioner needs to make every effort to ensure the accuracy and integrity of the investigation is maintained. The compilation of a jargon free report is integral to the dissemination of the findings from the investigation. This report should be compiled so that it is comprehensible by all stakeholders whatever their background. The practitioner should aim not to include words and terms that are familiar only to persons from a technical background.

The reporting phase of the digital forensics process may, like other forensics fields, involve the practitioner having to give testimony in court. Being an expert witness will require that practitioner be able to fully explain and justify the findings of the investigation to jurors and other members of a court. This is an additional reason why the final report should be jargon free and understandable by all.

4.3 2IR Designs Testing

The initial survey findings led to the development of a framework of standards and methodology that included particular missing elements identified from the survey paper and the review of relevant literature. Following the creation of the 2IR framework of standards and accompanying methodology there was need to have them validated. An overview document was developed along with a set of ten (10) interview questions directly related to the framework and methodology. They were later sent the developed mobile application and four additional questions directly related to this 2IR application. These questions were designed to gain valuable feedback from practitioners on the developed designs. The main objective of this exercise was to ascertain the validity of designs in a practical setting and the usefulness of having a mobile application. The target audience for this exercise was digital forensics practitioners from the different backgrounds including legal, law enforcement and technical. The participants were encouraged to be liberal in their responses and not hesitate to say exactly as they felt and to be expansive on their answers. The research engaged the use of electronic interviews. Electronic interviews refer to interviews held in real time facilitated by using the internet (Morgan and Symon 2004). The group includes the use of VOIP such as Skype, Google plus hangouts and Facebook as well as email interviews and the use of chat rooms and forums. Such methods of interviewing present an advantage when the interviewees are widely dispersed geographically. The use of electronic methods to interview participants also reduces the need for manual recording of interviews.

The interview questions and analysis

Thirty one practitioners were selected to be interviewed for this phase of the research some electronically. (A sample size of thirty or more (z) are deemed to be more reliable (Miles and Huberman 1994) The only demographic data taken was their region in an effort to preserve anonymity (due to the small sample size). The sample included six (6) practitioners from the United States including three from a technical background, two academics and 1 practitioner from a legal background. There were six (6) British based practitioners, four academics and two from a purely technical background. The sample group also included eleven (11) practitioners from the Caribbean that had one forensics accountant, two academics, one lawyer (who is certified digital forensics personnel), three practitioners from a technical background and four law enforcement officers. In addition there was a group of practitioners in a category labeled ‘rest of the world’ that included two (2) technical practitioners from India, three (3) law enforcement personnel for Europe (one from Europol), one (1) practitioner of a technical background from Australia and two (2) law enforcement officers from the Middle east. The participants were all known or recommended by other practitioners. Seven of the interviews arrangements took place at a related conference attended by the researcher.

The design documents, a copy of the 2IR frame work and methodology along with a link to the proposed interview questions were sent to a group of twenty three (23) (the other eight (8) were done at a conference) known or recommended digital forensics practitioners and the preferred electronic method of interviewing such as; Google Hangout, Skype or Facetime contact was arranged. A website and blog was also created to facilitate easy access to the designs and their description by practitioners. Participants were also encouraged to email further thoughts to the researcher following the interview should they wish to do so. While some of the practitioners had participated in the initial survey there were others who had not. Some participant practitioners had offered themselves after visiting the website and/or blog after it was placed on Google plus and twitter.

As with the survey respondents, the interviewees agreed that the field of digital forensics did need a framework of standards to guide practitioners carrying out the process. Transcript of the interview questions may be found in appendix E.

The researcher sought to find out if the designed methodology covered the details required in the field by practitioners and if there were practically applicable in the field. Practitioners were asked:

Does the methodology cover the details necessary for an investigation?

All respondents indicated that the 2IR framework of standards did cover the all the core facets of digital forensics process namely legal, technical, education and ethical. All interviewees indicated that the framework was indeed flexible and open enough to be applicable to the different variants of digital forensics including but not limited to mobile, cloud and network forensics. The nature of the standards/policies developed made them applicable without need for modifications.

The interviewer sought to ascertain if there were any changes that an interviewee would make to the framework to make it more applicable in the jurisdiction/s in which they worked.

*Would you make any changes to the 2IR methodology? *If yes, what would you change and why?*

All the interviewees indicated that they thought the 2IR framework was general and flexible enough to be used in their jurisdiction without any changes.

The research first sought to gather opinions with respect to the scope of the methodology, whether or not it covered all the important steps as perceived by practicing digital forensic personnel. All interviewees indicated that they thought the 2IR methodology did cover the steps and detail necessary to have a successful digital forensics investigation. One practitioner expanded on his response by saying that, the 2IR methodology did involve more steps then he and his team usually engage in, it did cover the relevant steps.

To ensure that the 2IR methodology was not overly theoretical and seen as just another academic finding practitioners' thoughts were sought on the methodology being applicable to real world investigations. *Would this methodology be applicable to the real world of investigations?*

The responses were all positive with answers ranging from, ‘yes’, ‘of course’ to ‘sort of’. As a follow up to this question and in an effort to promote the acceptance and use of the 2IR methodology in the field interviewees were asked if they would adapt the methodology for use in their organizations and if so what changes they would make in doing so. *Would you adapt this methodology for use in your organisation? *If no please say why not.*
Most of the interviewees said they would use the methodology without any changes with five indicating that they did not already have one in place and thus the 2IR would prove quite useful to them. Ten of the interviewees suggested that they would require more detail to the 2IR methodology before adapting it for use in their practice. Two practitioners specifically noted that they would require more specific steps throughout the investigative phase prior to adaptation as this is the area in which they required most help. One practitioner stated that he would have modified steps three, four and five of the investigative phase for use with mobile forensics as there were procedures that were different in his practice during this phase.
Another practitioner noted that he would not have used the 2IR methodology for investigations in his firm because “I have no idea how it can be implemented in real life. I need an instantiation for a real scenario as an example. There are a lot of intricacies in each step that I have no idea how it can and will be addressed”. To the follow up question he noted “It is abstract enough to cover the general steps covered in a digital forensics investigation”. This was then followed up with the participant providing more information on the 2IR methodology and framework along with a case study.

Following this the research then sought to determine the applicability of the 2IR framework to an e discovery setting. *Do you think this methodology is flexible enough to apply to an e-discovery setting as is?* Participants were given the option of forgoing this question and thus all but four interviewees opted respond to this question. Of the four interviewees two agreed that the methodology is flexible enough to be applied in the e-discovery setting. One practitioner said he didn’t think it covered it adequately while the other responded: “I am sure it could be adapted for e-discovery”. The results from this question were deemed inconclusive as there weren’t enough responses from the interviewees.

The need for standards in digital forensics cannot be overstated and thus the research sought to ascertain the views of practitioners on this need. *Do you think a framework of standards is necessary to guide a Digital forensics investigation? *Yes/No - Please give reasons for your answer.*

Twenty nine of the thirty one interviewees in their response said yes there is need for a set of standards in the digital forensics field to guide the digital forensics process. Specific responses included but were not limited to; “Yes, but they should be based on the specific legislative issues for the respective countries”. “Yes, digital forensics is fairly new and thus strict guidance is needed especially in the legal and ethical areas. One practitioner noted that he thought that such a framework already existed and cited the example ‘www.digital-forensics.org’. The researcher/interviewer being familiar with the ‘Digital Forensics Framework (DFF)’ hosted by the listed URL noted to the interviewee that this framework is actually a programming platform for the development of digital forensics tools which was not an objective of this research. The interviewee noted this and the interview continued.

The research then continued to ascertain if the framework adequately covered the facets of digital forensics field that it aimed to. *Do you think the 2IR Framework covers the legal technical ethical and educational areas necessary for personnel dealing with digital evidence?*

One practitioner’s response was: ‘Yes, a bit more legal stuff could have been included such as specific laws that will prove to be an issue throughout any investigation’. The framework has since been amended to include this suggestion. Other responses included; ‘Yes, Much more than needed’, ‘Yes, especially like the education standards’ and ‘Yes, it’s a good idea to place the standards under the different facets’.

One of the main objectives of this project is to produce a framework of standards with an accompanying methodology that may be used as a bench mark by practitioners in different jurisdictions worldwide. It is with this in mind that the interviewer proceeded to ascertain whether or not there was anything that practitioners thought could be done to make the designs more applicable to their specific region. . *Is there anything that you think could be done to make the Framework more applicable to your region?*

Six of the interviewees said no, there was nothing they needed to do as the designs were flexible enough to be adapted to their specific settings. Other response included, accommodation to record equipment to be used should be specified, it could include checking of equipment to be used in the investigation during the initiation stage, while one practitioner suggested that the legal issues be tied in with the ethical components.

4.3.1 Summary of Test findings

This section presents the themes emerging from the interview with practitioners in the field. The interview followed the exposure of practitioners to the developed designs and revealed the following findings:

1. The designs tested did cover the facets set out in the objectives. The designs of the 2IR Framework and Methodology did cover the indicated core facets of the digital forensics field as outlined in the objectives of the research.

2. The designs are flexible and adaptable to the different existing variations of digital forensics with regards to types of devices such as mobile forensics, cloud forensics, network forensics and can be used across different jurisdictions worldwide (UK, Caribbean, USA, Europe etc).

3. The language used in the designs make it useable by practitioners from different professional background with different levels of training. There was no use of subject specific jargon (Legal or Technical).

4. A number of practitioners were either not aware or totally unconcerned about issues related to e-discovery. Electronic discovery, like digital forensics, has many definitions (Biggs and Vidalis 2009) defines e-discovery (as it is referred to) as being any process in which electronic data is sought, located, secured with the intent of using it as evidence in a civil or criminal case. Electronic discovery refers to locating electronically stored information on computers and other technologically related devices. This electronically stored information/data is used in court as digital evidence. It is therefore important that digital forensics practitioners be cognizant of the intricacies involved in e-discovery.

The main objective of this research project was to produce designs that would better help practitioner in the field carry out their duties in a more standardized format. To promote more commonalities in the field with regard to collecting digital evidence. Digital evidence has become quite critical to the legal framework and thus there needs to be some uniformity in how it is acquired and handled.

The findings of the research indicated there is indeed some disjoint within the field that there is need for the creation of standards similar to other forensics fields and types of evidence to ensure that digital evidence is viable when presented in court. The research identified several short comings in the digital forensics field and seeks to address them through the 2IR framework, methodology, app and training programme.

The findings from the data gathered led to the development of designs to address the issues identified. The designs which are presented in the following chapter include a framework of standards which consist of a set of principles arranged against the phases of the digital forensics process (Initiation, Investigative, Reporting) and according to the four core facets of the field (Technical, Legal, Educational, Ethical). These designs also include a curriculum of studies addressing the need for trained personnel in the field of digital forensics. The designs which are presented in the following chapter also include a mobile application replicating the steps from the methodology and guided by the legal and ethical principles of the framework.

The results from this study/research will prove useful to policymakers, educators as well as practitioners the associated backgrounds as they work to construct viable programmes addressing the need for growth in the digital forensics field.

CHAPTER FIVE

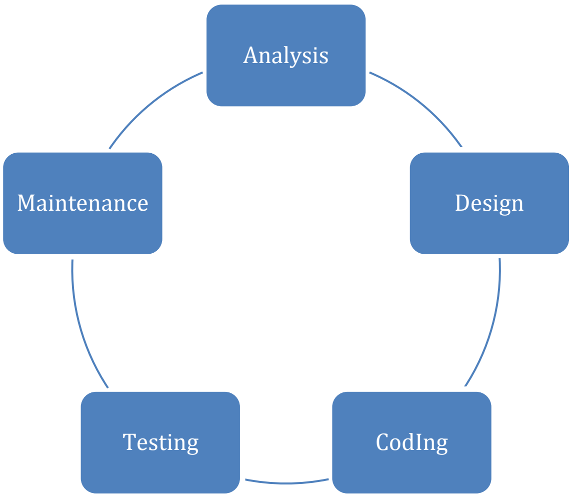
The 2IR Mobile Application

5.1 The 2IR Mobile Application Introduction

Digital forensics tools are critical for the digital forensics industry and without them a cybercrime or computer crime investigation cannot be carried out. These tools are designed to carry out different purposes throughout a digital forensics investigation and have, for the most part, been reliable in producing digital evidence that have been used in courts for various types of cases. There are a number of digital forensics applications available to practitioners for use in mining and analysing data. These may come in the form of the tools as described earlier in this chapter well as in the form miniature app such as a mobile application. Research revealed one digital forensics mobile application tool developed by private companies for use with their main stream applications, MPE+ by access data.

This section provides an introduction to the application tool (2IR APP) developed specifically for this study. The application developed for this project is not a mining or analysis tool/application and does not perform the functions of the applications described earlier in this chapter. The 2IR mobile Application focuses on the procedural aspects of the digital forensics process highlighting the legal and ethical principles of the investigation. Being founded on the four core facets of the field it assures the production of reliable and verifiable digital evidence.

The development of this application followed the waterfall model of system development lifecycle.



5.2 Analysis Phase

The 2IR mobile application is an accompaniment to the 2IR methodology guiding the practitioner through the digital forensics process assisting the practitioner to ensure that there is adequate maintenance of the chain of custody and continuous observance of the legal issues. The application provides convenience and mobility instead of digital forensics practitioners having bulky paper guidelines or electronic document to refer to each time, the application can be conveniently located on the practitioners preferred electronic/mobile device for use in the field.

What the systems does

The 2IR mobile application is created to follow the steps of the 2IR methodology providing guidance electronically to the practitioner throughout a digital forensics investigation. It assists the practitioner in ensuring that there is adequate maintenance of ethical conduct and observance of the legal facets of the field. The 2IR mobile application being a part of the 2IR designs is also governed by the 2IR Framework of standards and falls within the remit of the stated standards and policies.

Who will be using this system?

The system is designed for use by Digital forensic practitioners from varying different backgrounds including: Law enforcement officers, private investigators, IT personnel within an organizations as well as legal personnel involved in conducting digital forensics investigations.

This application is designed to accept inputs given and produce intermediate output (on screen). This system is secure, easy to use and user friendly. Inputs will be accepted as indicated on the screen when prompted, with an on screen report produced at the end of the first two phases. The user should not be allowed to proceed to the next phase unless the previous phase is complete. They should also be able to recall any already entered data at anytime and change it. This should be reflected in the output screen.

The 2IR Application is developed using HTML, Ajax and Javascript. It has been designed and tested for use in the Internet Explorer and Google Chrome on Windows based machines as well as in Safari Browser on Mac computers. It has also been tested for use on mobile devices iPad, iPhone and Samsung Galaxy. The database used to support its development is MySql.

Screen One (1)

The Sleep state (landing page) of the application shows an overview of the application describing how it falls under the 2IR framework of standards and the features of its design.

See screen shot of The Landing Page of the 2IR mobile Application in Testing section

Home Screen

The home screen of the application upon startup will present a screen showing the name of the application and its use. There is no user interaction at this stage.

See screen shot The Home Screen of the 2IR Mobile Application in the testing section.

Log in Page

The Home screen is followed by a page that requests input in the form of alpha numeric text for practitioners name and number as well as their user name and password. This page has been designed to ensure secure entry into the application.

See screen shot of User Data collection screen in the testing section

After entering their details the practitioner then submits the data following which the case and general data capture screen will be presented onscreen.

Case General Data Capture Screen (Requester Data Capture)

After logging in the practitioner will then capture the basic details of the request. This data will include assigning a case number and name, capturing the name of the requesting organisation, the type of service required, the date and the type of legal authrisation that will be required. Data to be captured at this stage also includes a contact name from the requesting organisation preferably the initial contact person as well as the location or locations of the intrusion/incident.

See screen shot of Requester Data Collection Screen in the testing section

Upon entering the basic details of the request, the practitioner after noting the type of legal authorisation that will be required, the practitioner then submits to continue to the next screen, phase one which will prompt the appearance of the next screen.

Phase 1 – The Initiation phase (I)

The login screen is followed by the first phase (I-Initiation) of the application which follows the steps of the 2IR Methodology. It guides the practitioner ensuring that critical administrative steps as outlined in the methodology are followed. At this phase particular basic information captured before will be regenerated including the practitioner name and number as well as the requesting organization. The main objective of the initiation phase is to set the stage for the rest of the investigation by assessing the situation and collecting relevant data to ensure that the necessary actions are taken and the needed documents are produced before actual search, seizure and investigation begins. Inputs to the application at this stage include;

1. Case Identification: this will be unique alpha numeric character indentifying the case being investigated. This alpha numeric character will be randomly generated and regenerated for each screen to come. .

2. Practitioner/s Name and Number (Reproduced from previous screen)

3. Organisation (Requesting) This information is reproduced from the previous data collection step.

4. Date of request - this phase will include the reproduced date of original request as well as the current date when the phase is being carried out.

5. Assessments - This section of the application serves also as a reminder of the steps to be covered by the practitioner. It guides the general assessment of the situation with regards to the scope and intent of the investigation. The practitioner in this case checks the box indicating completion of the tasks indicated.

a. Personnel Assessment. The practitioner will check this box after an assessment is done of all persons who are connected or possibly connected to the incident. This include people who are aware or involved in the incident as indicated in the 2IR methodology.

b. Data Assessment- The practitioner checks this after estimating the amount of data that will be involved and ascertaining where the relevant data may be found. This is very critical to the investigative phase as the practitioner will need to know if contact is to be made with persons outside the immediate remit of the requesting party.

c. Device assessment - this is checked when the practitioner is satisfied that all relevant devices that may have been involved in the incident are identified.

After completion of all the tasks required for this section of the application, the practitioner checks the boxes and moves on to the next step.

6. Risk Analysis This particular section helps the practitioner in determining if the case is feasible. The practitioner needs to ensure that all the necessary resources are in place to carry out the investigation. This includes both human (skills) resources and tools (hardware and software).

At this point the application collects data on ensuring that the three types of risk analysis has been completed. The practitioner will record the relevant data and information on the appropriate form as indicated in the appendices and check in the appropriate boxes.

a. General Risk Analysis

b. Personal/ Practitioner Risk Analysis

c. Requester/Company Risk Analysis

After completion of the above analysis, the practitioner checks the boxes and moves on to the next step in the phase.

7. Legal Permission - The legal aspects regarding the investigation should be established before any search, seizure or actual investigation begins. This tab reminds the practitioner of the need for legal authorisation and ensures that the practitioner cannot move to the next stage of the investigation without it being completed.

8. Create plans - After completion of collecting the data necessary for the start of the investigation the practitioner then proceeds to creating a strategic plan of action which will form an important part of a defensible audit trail.

At the end of the phase the application reminds the practitioner of the need to complete the steps indicated and it also provides a chance for the examiner enter any task that is not completed.

As noted before the 2IR application guides practitioners through the digital forensics process. At the first phase the application will guide the practitioner through the data items that need to be collected to ensure successful completion of the first phase and to prepare for the second phase. It ensures adherence not only to the methodology but also especially to the legal issues.

See screen shot of Phase 1 Data collection screen in the testing section

The application prompts the user to either continue to phase two or enter the missing task/s that need to be revisited before continuation. Upon successful completion of this phase the practitioner will be authorized by the application to continue to the next phase of the process.

Phase 2 The Investigation Phase (I)

Following completion of the first phase of the 2IR Methodology via the 2IR Application the second phase then comes onscreen. The Case identification, Practitioner's name and number along with the date of request are then reproduced from the previous phases.

The new inputs accepted throughout this phase include;

-Date: This Date refers to the date the phase begins as opposed to the date of request that is reproduced. This helps in the chain of custody.

1. Physical Image of scene captured Y/N

- Drawing a physical sketch of the scene to include all physical devices electronic and otherwise should be captured in this drawing. It must be clear enough to be read by others.

- Digital camera the use of a digital camera to capture the scene can be quite useful as the practitioner is able to look and ensure that what is on the camera is a true reflection of the particular scene at which one is present.

-Notes - The scene may also be captured in writing by the practitioner noting what was found where.

-Other – Other methods of capturing the incident scene are further explored in Section 5.2.

The application will prompt the practitioner/user to enter whether or not a physical image of the incident scene has been captured. The application then provides input boxes for the entry of how the scene was captured.

2. The application then moves onto prompting the user to enter the amounts and names of suspect devices identified in the initial assessment.

Suspect devices identified Y/N

Name of Devices	Number
1.	
2.	

The application then allows for the users to enter data integral to the investigation including: Live data captured, devices removed to controlled area, static data captured, Data Mined, Live data preserved, static data preserved, data analysed. These are entered as a response to questions via checkboxes.

The 2IR application also facilitates the entry of data on the tools used. Here the practitioner will make a note of the tools used throughout the investigation

See screen shot of Phase two data collection screen in the testing section

Phase 3 The Reporting Phase (R)

This is the final section of the application as dictated in the methodology. This phase is totally dependent on completion of the previous phases.

It reproduces data including case identification, requesting organization, date of request and practitioners details. Further it accepts the following inputs prompting the user to enter whether or not they have created the necessary inventories as dictated by the 2IR methodology. Starting immediately after the extraction and analysis of evidence this phase will guide the practitioner in organising the evidence with the first step being to create inventories of all items used throughout the investigation. This will be entered as responses via checkboxes.

Inventory Created

Hardware Devices Y/N

Software Devices Y/N

Additional Items Y/N

The reconstruction of the incident scene helps in establishing exactly what happened when, how and by whom. It helps to clarify any issues with the examination and analysis of the evidence found. This is also included in the application to be checked off by the practitioner.

- Reconstruction of Crime Scene Done Y/N

The creation of an intruder/suspect profile assists the practitioner in a number of ways including that of reducing the number of suspects in a case making it easier to trace and identify the perpetrator of the incident.

- Intrusion profile created Y/N

The remaining checks are administrative checks as indicated in the 2IR methodology ensuring completion of the reporting stage before exiting the application.

Archive Done Y/N

Report Completed Y/N

Report Checked Y/N

Report Submitted Y/N

Phase 3 Completed Yes (end of Investigation) No (enter missing task)

Analysis summary

This system is to be designed for use on a desktop computer, tablet or smartphone providing the convenience of having guidance for the digital forensics process on hand. At the end of a complete forensics investigation it is capable of producing a miniature report of the investigation. The intention of the application is not to mine and analyze data but to guide the process (as in the 2IR Methodology) ensuring adherence to the ethical, and legal standards as outlined in the 2IR Framework.

The deliverables presented in this research are a result of in-dept research and analysis of results from related surveys and interviews. The employment of a variety of research methods and the presentation of the initial designs to professionals in the field for testing to ensure that they are not merely superficial and theoretical but that they are applicable to the field of practical work and are suitable for use by working practitioners.
These designs are also the result of an in-depth investigation into the various designed methods used to acquire digitally stored data/information that is used as evidence in courts.

5.3 Design Phase

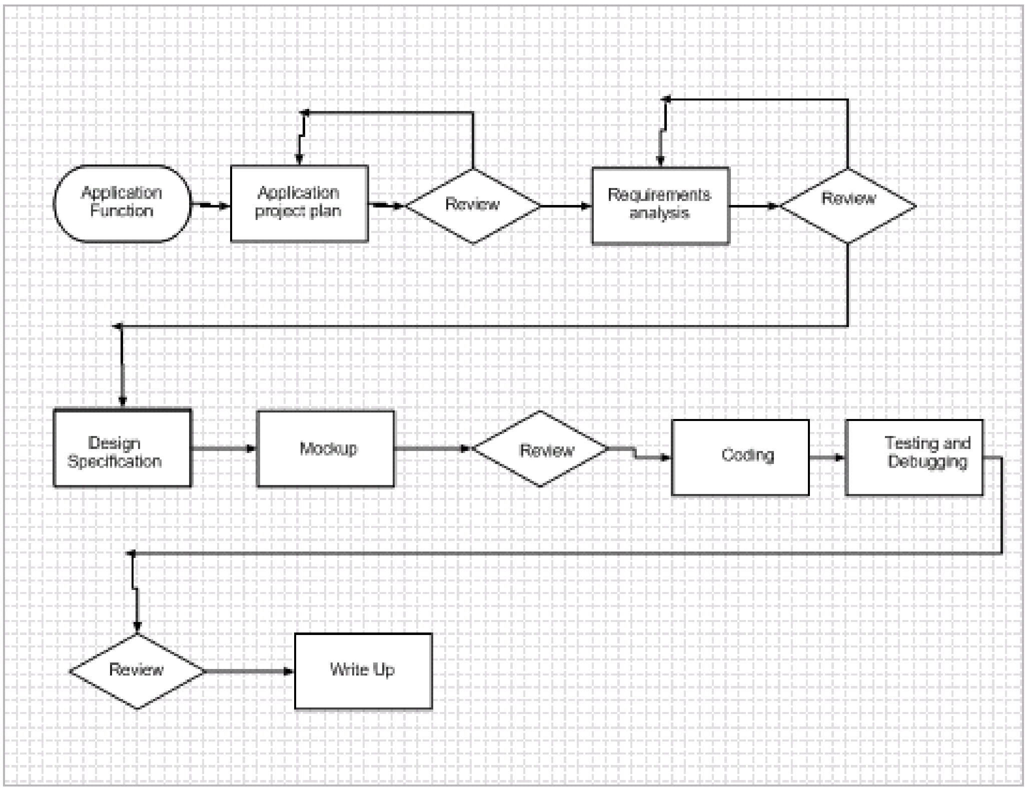


Figure 5.1 Overview of the process taken by to produce the 2IR mobile application

5.3.1 General Flow of the system

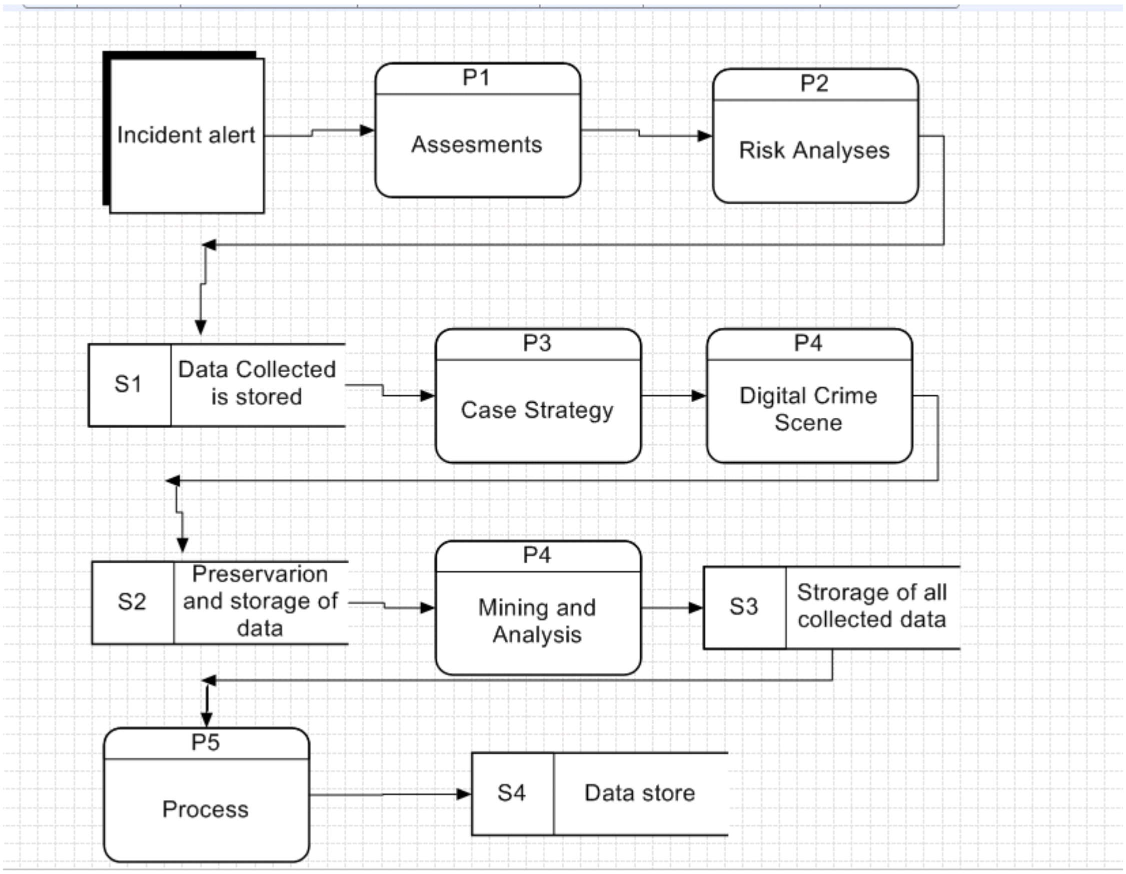


Figure 5.2 Chart depicting general overview of the 2IR methodology to be followed by the mobile application.

5.3.2 Stage 1

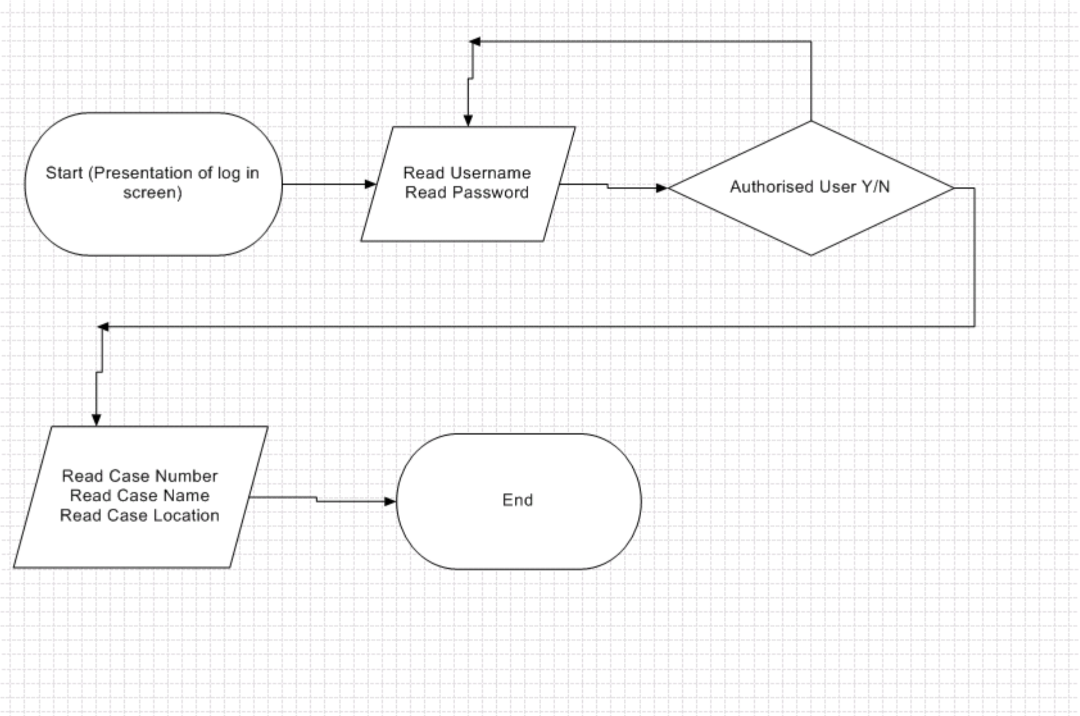


Fig 5.3 Diagram showing the flow of data on the initial screen of the mobile app.

5.3.3 Phase 1

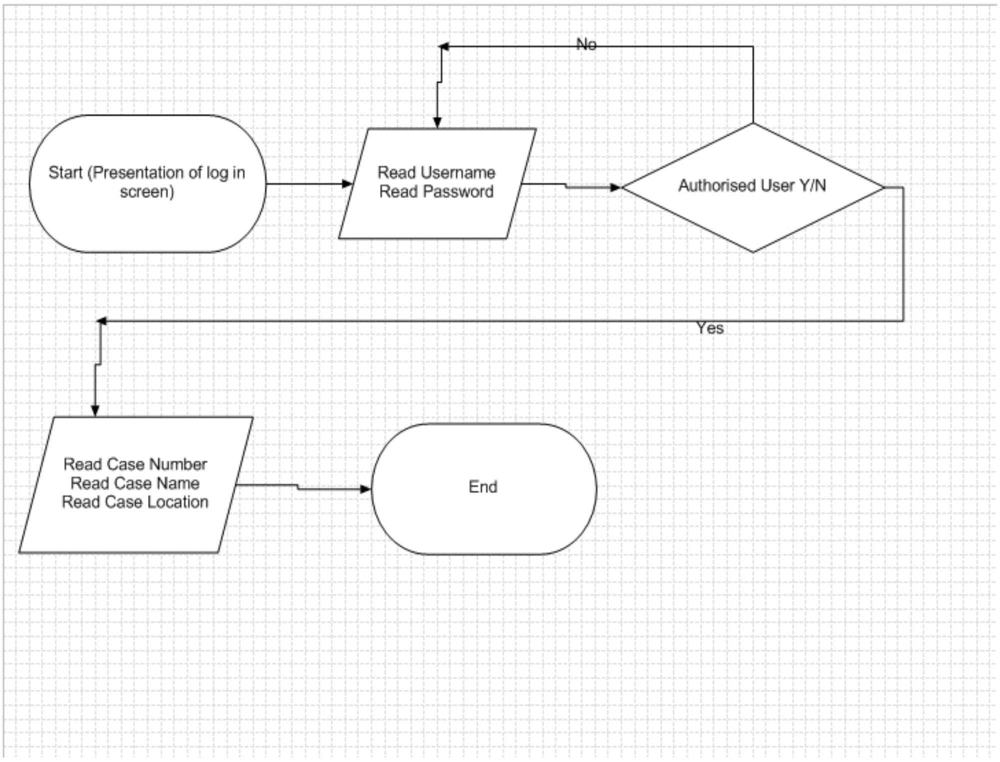


Figure 5.4 Flow diagram of the first phase of the mobile application app.

5.3.4 Phase 2

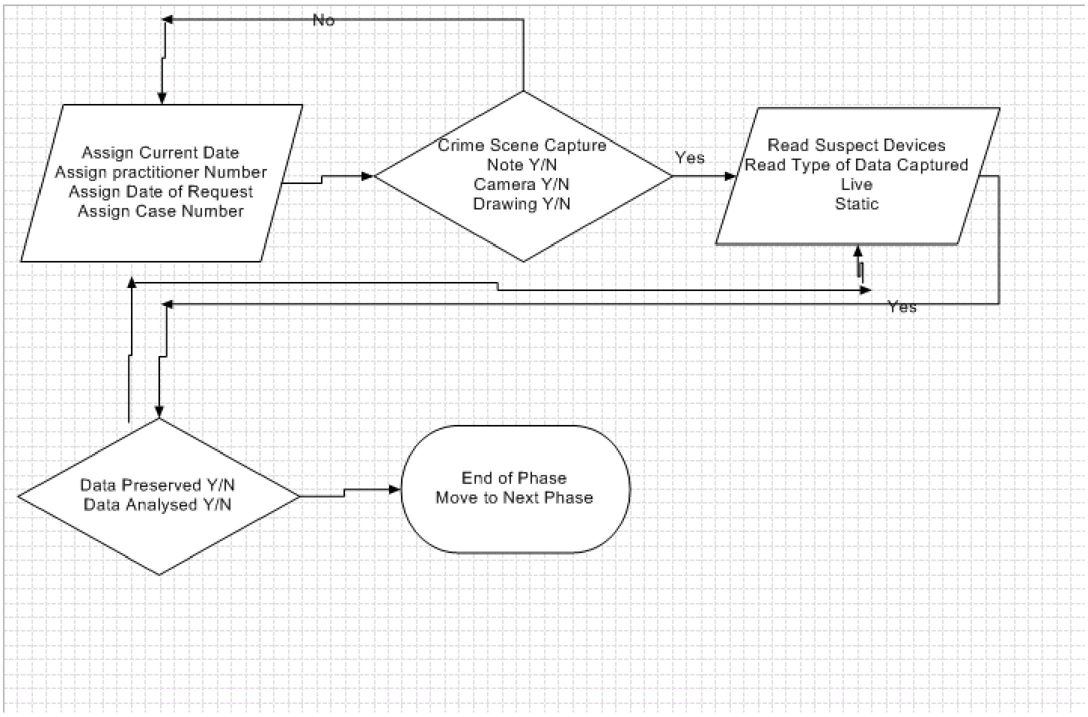


Fig. 5.5 Diagram showing data flow of the second phase of the Mobile app.

5.3.5 Phase3

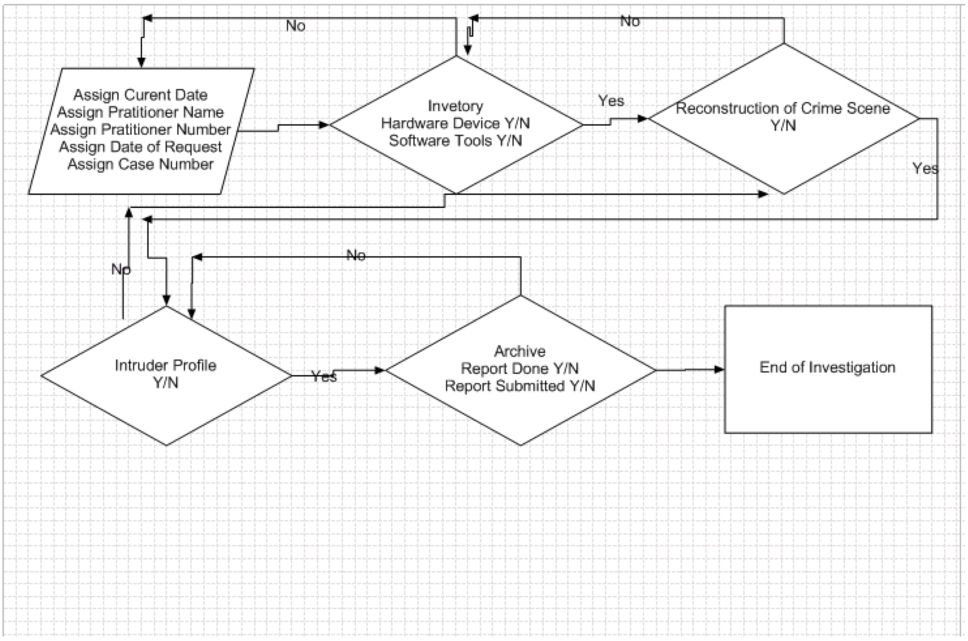


Fig 5.6 Flow Diagram of the final phase of the 2IR Mobile application

5.4 Coding

This section presents the initial set of codes for the 2IR mobile application.

Landing Page

```
<!DOCTYPE html>
<html>
<body>
<div id="container" style="width:500px">
<div id="header" style="background-color:#0000FF;">
<h1 style="margin-bottom:0;">The 2IR Methdology</h1></div>
<div id="header" style="background-color:#FFFF00;">
<h3 style="margin-bottom:0;">Facets:    Technical(T) Legal(L)  Education (E)Ethical (E1)</h3></div>
<div id="menu" style="background-color:#FFFF00;height:200px;width:100px;float:left;">
<b>Phases</b><br>
Initiation (I1)<br>
Investigative (I2)<br>
Reporting (R)</div>
<div id="content" style="background-color:#00FF00;height:200px;width:400px;float:left;">
The 2IR methodology has three major phases ( described in the framework) that will be further broken down in to more specific steps.  It is designed to be prescriptive and rigorous while ensuring speed and accuracy.  It is prescriptive because it will include recommendations of the use of particular tools at different stages in the process and is guided by standards.  It is rigorous because it is expected that no phase will be excluded. This measure ensures the model is accurate and reliable.  Educational training and qualification along with legal and ethical principles encompass the methodology.</div>

<div id="footer" style="background-color:#0000ff;clear:both;text-align:center;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>

</div>

</body>
</html>
```

Idle page

Login Page

```
<htm4>
<body>

<h1>2IR Digital Forensics </h1>
<body style="background-color:yellow;">

<form>
Practitioner Name: <input type="text" name="firstname"><input type="text"
name="lastname"><br>
PractitionerNumber<input type="number" number="PractitionerNumber">
<br>

</form>

<form action="demo_form.asp">
 Date (date and time): <input type="datetime" name="daytime">

</form>

<form name="input" action="html_form_action.asp" method="get">
UserID: <input type="text" name="user">

Password: <input type="password" name="pwd">
<input type="submit" value="Submit">
</form>

<br>
<br>
<br>
```

```
<div id="footer" style="background-color:#0000ff;clear:both;text-align:left;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>

</div>

</body>
</html>
```

Case detail Page (Page 3Coding)

```
<htm2>
<body>
<div id="header" style="background-color:#FFFF00;">
<h2><center>2IR Digital Forensics</center></h2>

<p><b>Practitioner Name:    </b></p>
<p>Practitioner Number:   </p>

<form>
Requesting Organisation: <input type="text" Requester="Requester"><br>
Contact Name: <input type ="text" ContactName="ContactName"><br>

Type of Organisation: <input type="text" requester="requestingOrganisation"><br>
Location/s: <input type ="text" Location="Location"><br>
Date of Request: <input type= "date" Date of Request="date"><br>

<h4>Nature of investigation Requested</h4>
Criminal <input type="text" name="Criminal"><br>
Routine/Civil/eDiscovery: <input type="text" name="non criminal">

<h4>Investigation required</h4> <br>
<input type="checkbox" name="Yes" value="Yes">Investigation required<br>
<input type="checkbox" name="No" value="No">No Investigation Required
</form>
```

```
<h4>Legal Authorisation needed</h4>
<input type="radio" name="internal" value="internal">internal<br>
<input type="radio" name="External" value="external">external
<form/>
</body>
<body>
<input type="button" onclick="myFunction()" value="Continue to phase one (I1)" />
<div id="footer" style="background-color:#0000ff;clear:both;text-align:center;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>
</div>
</body>
</htm2>
```

Phase 1 The Initiation Phase

```
<htm5>
<body style="background-color: yellow;">
<h1>2IR Digital Forensics</h1>
<p>Practitioner Name:     </p>
<p>Practitioner Number:   </p>
<p>Case Number:  </p>
<form>
<h3>Phase 1 - Investigative (I1) </h3>
<h4> Assessments complete?</h4>
<p>Data Assessment</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<p>Pesonnel Assessment</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<p>Device Assessment</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
```

```
<h4> Risk analysis complete?</h4>
<p>General Risk Analysis</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<p>Personal/Practitioner Risk Analysis</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<p>Requester/Company Risk Analysis</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Legal permission been acquired?</h4>
<p>legal Authorisation</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<p>Type</p>
<input type="checkbox" name="answer" value="Yes">Warrant
<input type="checkbox" name="answer" value="no">Permission<br>
<p><b> NB. all analysis and assessments must be complete before the investigation
continues.  It is recommended that legal advice and authorisation be received before
any further are steps taken. </b> <br><br>
<h2>Phase 1 (I1) Complete?</h2>
<input type="checkbox" name="answer" value="Yes">Yes, Continue to phase 2 <br>
<input type="checkbox" name="answer" value="no">No Revisit(enter missing task):
<input type="text" name="user">
<input type="submit" value="Submit">
</form>
<head>
<script>
function myFunction()
{
alert("Do you want to continue!");
}
</script>
```

```
</head>
<body>
<input type="button" onclick="myFunction()" value="Continue to phase two (I2)" />
<div id="footer" style="background-color:#0000ff;clear:both;text-align:center;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>
</div>
</body>
</htm5>
```

Phase 2 Investigative phase

```
<!DOCTYPE html>
<div id="header" style="background-color:#FFFF00;">
<h2>2IR Digital Forensics</h2>
<p>Practitioner Name:  </p>
<p>Practitioner Number:  </p>
<p>Case Number: </p>
</form>
<h3>Phase 2 (Investigative) </h2>
<h4>Crime Scene Captured (Photo,drawing, etc)</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<br>
<h4>Methods used</h4>
<form>
<input type="checkbox" name="capture" value="Drawing">Drawing<br>
<input type="checkbox" name="capture" value="Digital Camera">Digital Camera<br>
<input type="checkbox" name="capture" value="Notes">Notes<br>
<input type="checkbox" name="capture" value="Other">Other
</form>
<h4>Number of Suspect devices </h4>
<form>
Suspect devices: <input type="number" name="suspectdevice/s"><br>
<h4>Live Data captured</h4>
<input type="checkbox" name="answer" value="Yes">Yes
```

```
<input type="checkbox" name="answer" value="no">No<br>
<h4> Devices removed to control area </h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Static Data Captured </h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Data Mined </h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Live data preserved </h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Static data preserved </h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Data Analysed </h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4>Tools used </h4>
<form>
Software Tools: <input type="text" name="firstname">
<input type="text" name="firstname"><br>
Hardware Tools: <input type="text" name="lastname">
<input type="text" name="firstname"><br>
</form>
<h3> Phase 2 (I2) Complete? </h3>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<form/>
<head>
<script>
function myFunction()
```

```
{
alert("Do you want to continue!");
}
</script>
</head>
<body>
<input type="button" onclick="myFunction()" value="continue to Phase 3 (R)" />
</body>
<div id="footer" style="background-color:#0000ff;clear:both;text-align:center;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>
</div>
```

Phase 3 Reporting

```
<!DOCTYPE html>
<div id="header" style="background-color:#FFFF00;">
<h2><center>2IR Digital Forensics</center></h2>
<p>Practitioner Name:     </p>
<p>Practitioner Number:   </p>
<p>Practitioner Number:  </p>
<p>Case Number: </p>
<h3>Phase 3 (Report Creation) </h3>
<form>
<h4>Inventory Created</h4>
<p>Hardware devices</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<p>Software</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<p>Additional Items</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No

<h4>Reconstruction of Crime Scene done</h4>
```

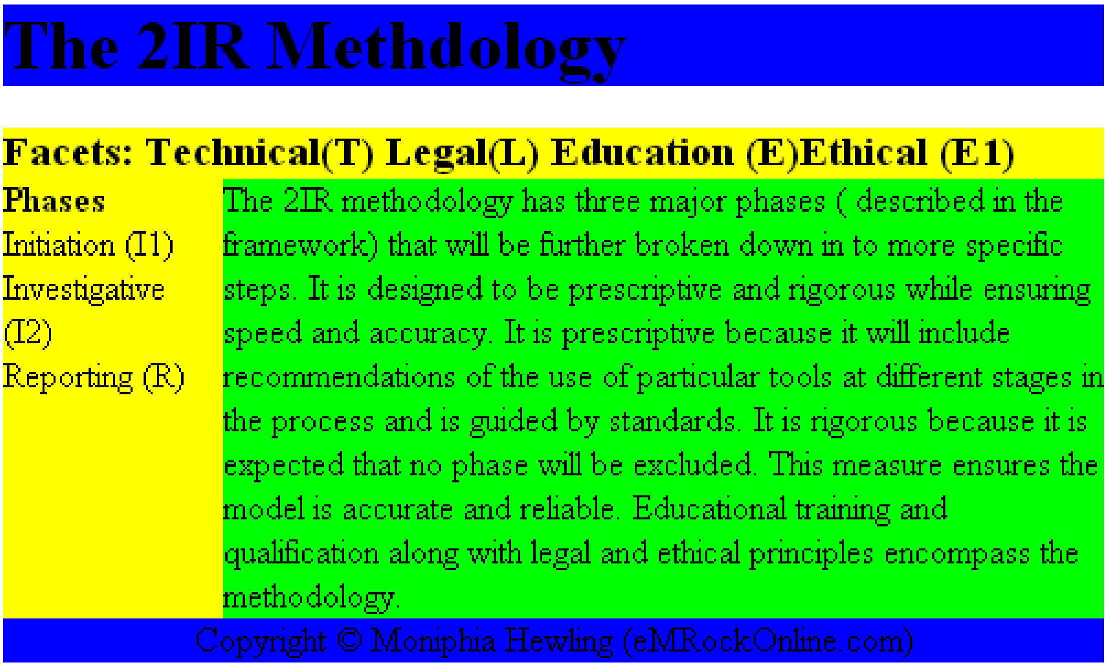
```
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No

<h4>Intrusion Profile created</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<h4>Archive done</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<h4>Report Completed</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<h4>Report Checked</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<h4>Report Submitted</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
</form>
<h2>Phase 3 (R) Complete?</h2>
<input type="checkbox" name="answer" value="Yes">Yes, End of Investigation <br>
<input type="checkbox" name="answer" value="no">No Revisit(enter missing task):
<input type="text" name="user">
<input type="submit" value="Submit">
</form>
<head>
<script>


<head>
<script>
function myFunction()
{
alert("Do you want to continue!");
}
</script>
</head>
<body>

<input type="button" onclick="myFunction()" value="End of Investigation (R)" />
<h4>Generate Investigation report</h4>
<input type="button" onclick="myFunction()" value="Click to Generate(G)" />
</body>
<div id="footer" style="background-color:#0000ff;clear:both;text-align:center;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>
End of investigation

<!DOCTYPE html>
<html>
<body>
<body style="background-color:yellow;">
<h1><center>2IR <center>Digital Forensics </center></h1>
<p>Thank You
<p>Practitioner Name:     </p>
<p>Practitioner Number:   </p>
<p>Based on your input to the 2IR Forensics Application the investigation is complete.
</p>



<h2><center>Thank you for using the 2IR App!!!</center></h2>

</body>
</html>
<div id="footer" style="background-color:#0000ff;clear:both;text-align:center;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>

</div>
```

5.5 Testing

This section presents results of the initial coding in the form of screen shots showing what the system will look like.

Screenshots of Application

Landing Page



The 2IR Methdology

Facets: Technical(T) Legal(L) Education (E)Ethical (E1)

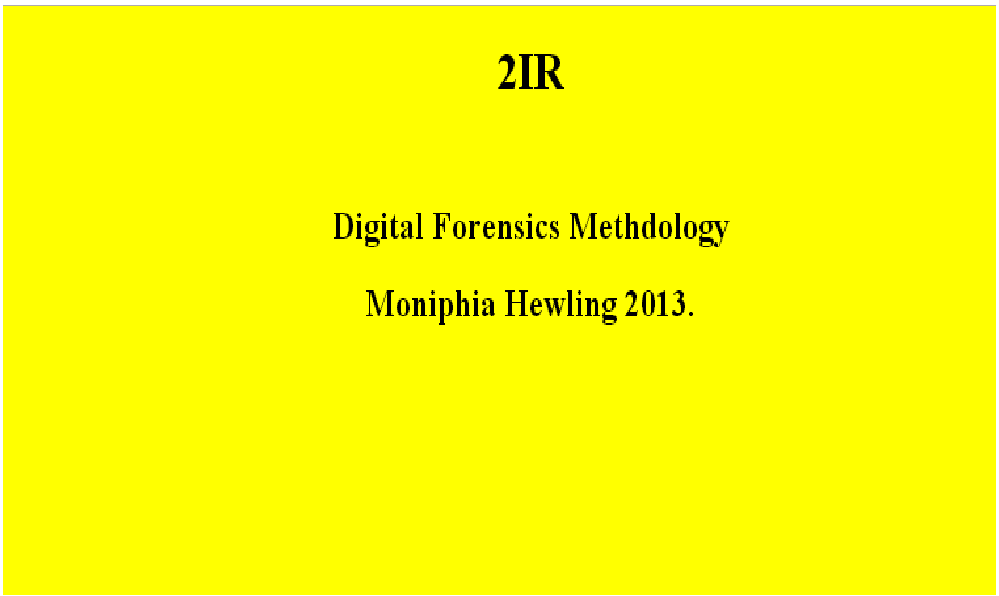
Phases
Initiation (I1)
Investigative (I2)
Reporting (R)

The 2IR methodology has three major phases (described in the framework) that will be further broken down in to more specific steps. It is designed to be prescriptive and rigorous while ensuring speed and accuracy. It is prescriptive because it will include recommendations of the use of particular tools at different stages in the process and is guided by standards. It is rigorous because it is expected that no phase will be excluded. This measure ensures the model is accurate and reliable. Educational training and qualification along with legal and ethical principles encompass the methodology.

Copyright © Moniphia Hewling (eMRockOnline.com)

The Sleep state (landing page) of the application shows an overview of the application describing how it falls under the 2IR framework of standards and the features of its design.

Screen Saver Screen



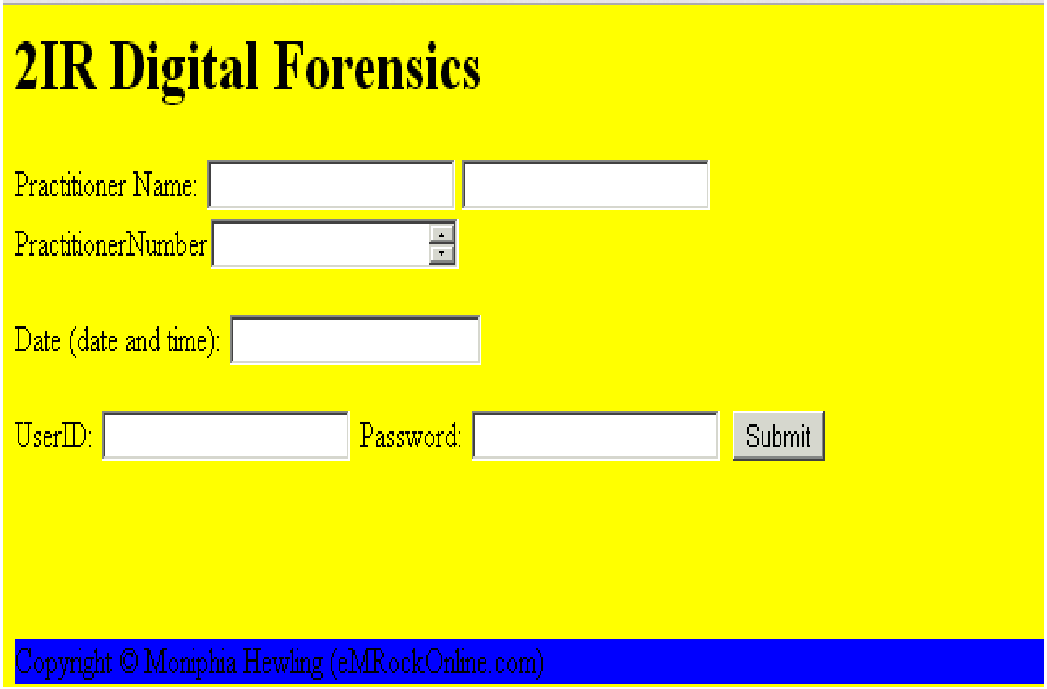
2IR

Digital Forensics Methdology

Moniphia Hewling 2013.

The home screen of the application upon startup will present a screen showing the name of the application and its use. There is no user interaction at this stage.

Log in Screen

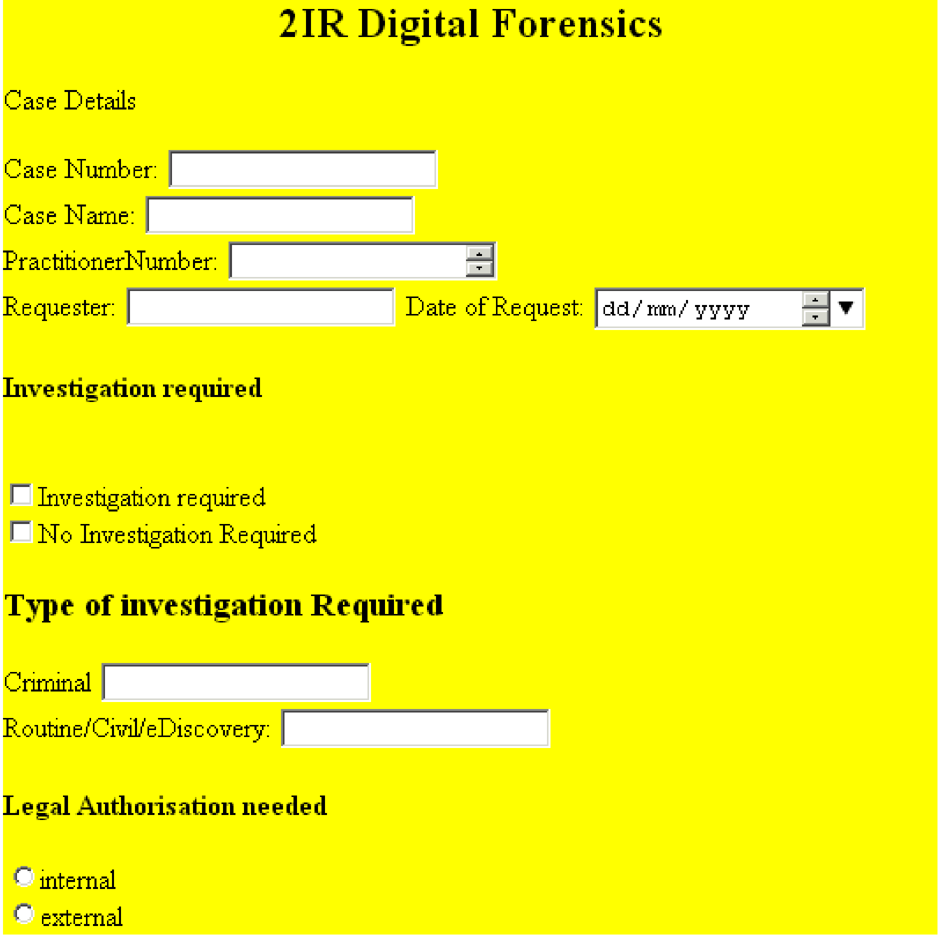


2IR Digital Forensics

Copyright © Moniphia Hewling (eMRockOnline.com)

The Home screen is followed by a page that request input in the form of text for practitioners name and number as well as their user name and password. This page has been designed to ensure secure entry into the application.

Case Detail Screen



2IR Digital Forensics

Case Details

Case Number:

Case Name:

PractitionerNumber:

Requester: Date of Request: dd/mm/yyyy

Investigation required

□ Investigation required
□ No Investigation Required

Type of investigation Required

Criminal

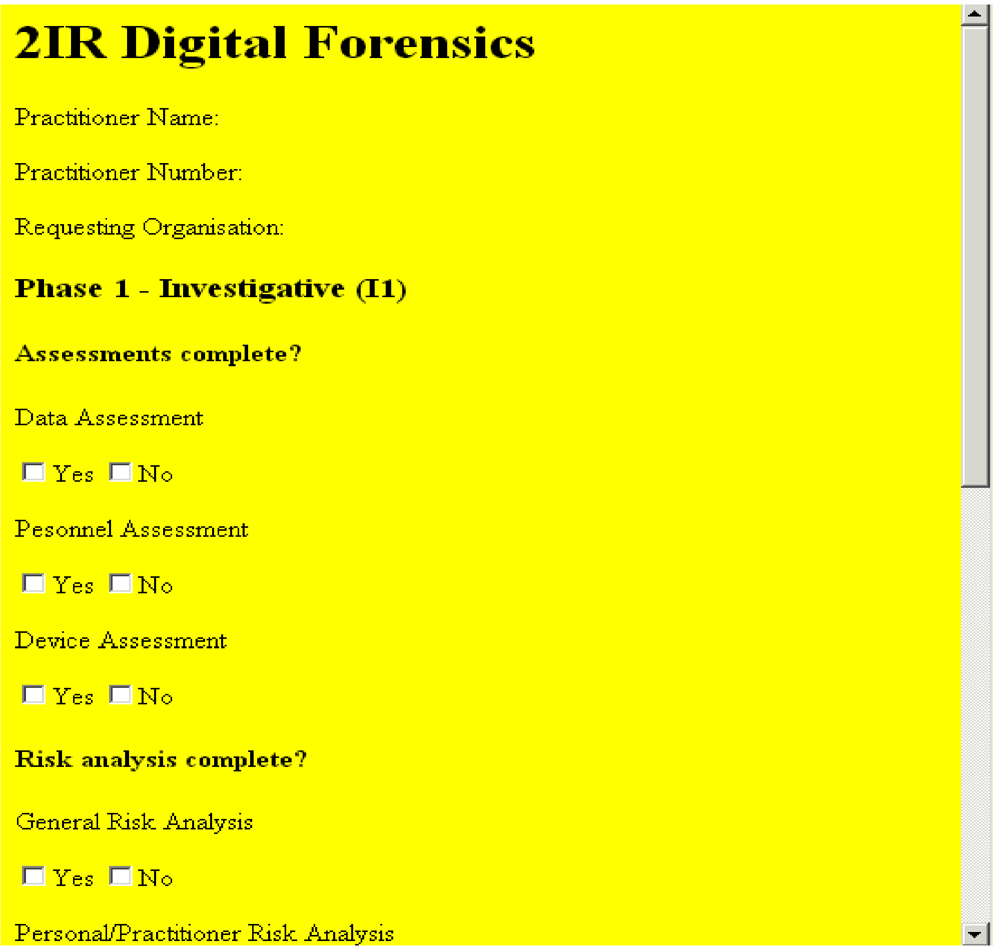
Routine/Civil/eDiscovery:

Legal Authorisation needed

○ internal
○ external

After logging in the practitioner will then capture the basic details of the request. This data will include assigning a case number and name, capturing the name of the requesting organisation, the type of service required, the date and the type of legal authrisation that will be required.

Phase one screen



2IR Digital Forensics

Practitioner Name:

Practitioner Number:

Requesting Organisation:

Phase 1 - Investigative (I1)

Assessments complete?

Data Assessment

□ Yes □ No

Pesonnel Assessment

□ Yes □ No

Device Assessment

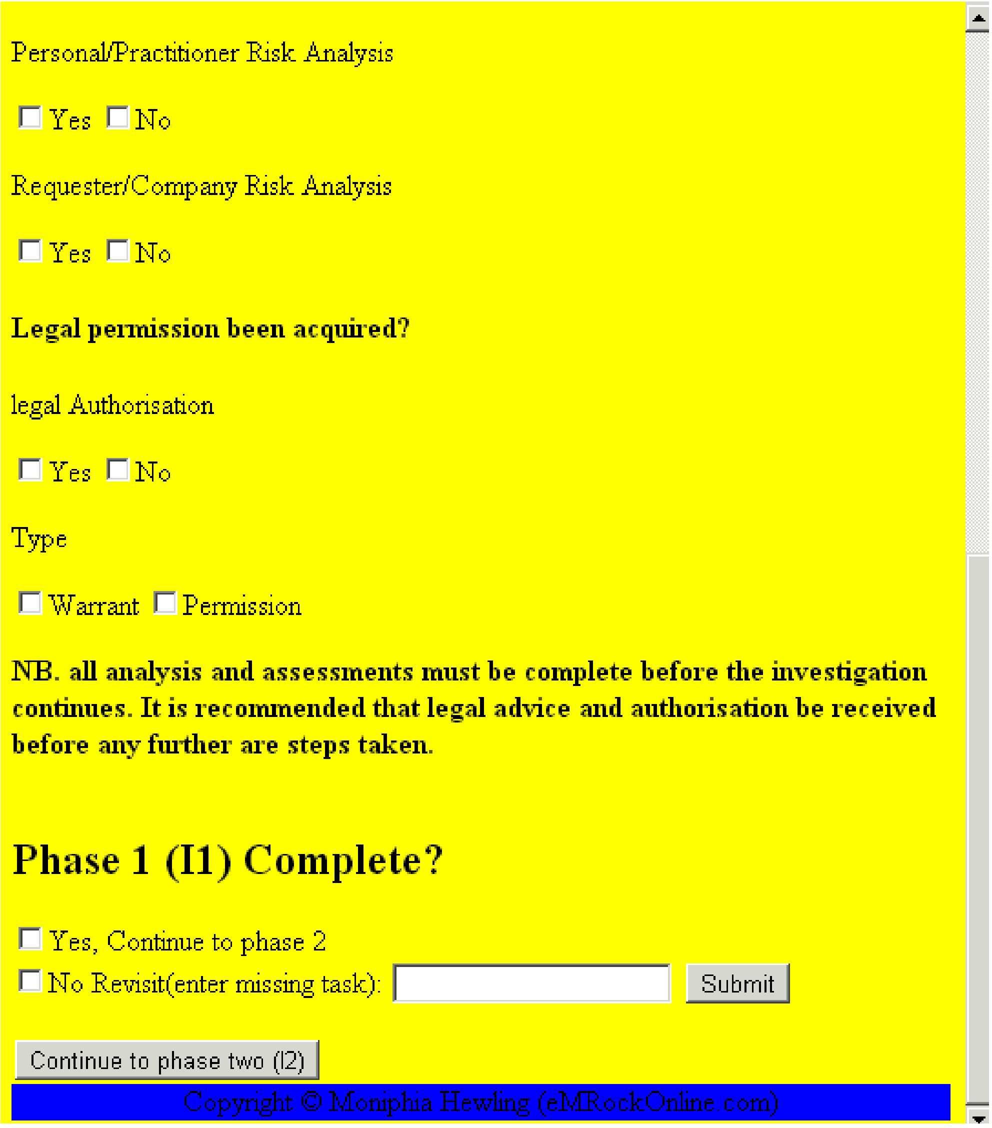
□ Yes □ No

Risk analysis complete?

General Risk Analysis

□ Yes □ No

Personal/Practitioner Risk Analysis



Personal/Practitioner Risk Analysis

□ Yes □ No

Requester/Company Risk Analysis

□ Yes □ No

Legal permission been acquired?

legal Authorisation

□ Yes □ No

Type

□ Warrant □ Permission

NB. all analysis and assessments must be complete before the investigation continues. It is recommended that legal advice and authorisation be received before any further are steps taken.

Phase 1 (I1) Complete?

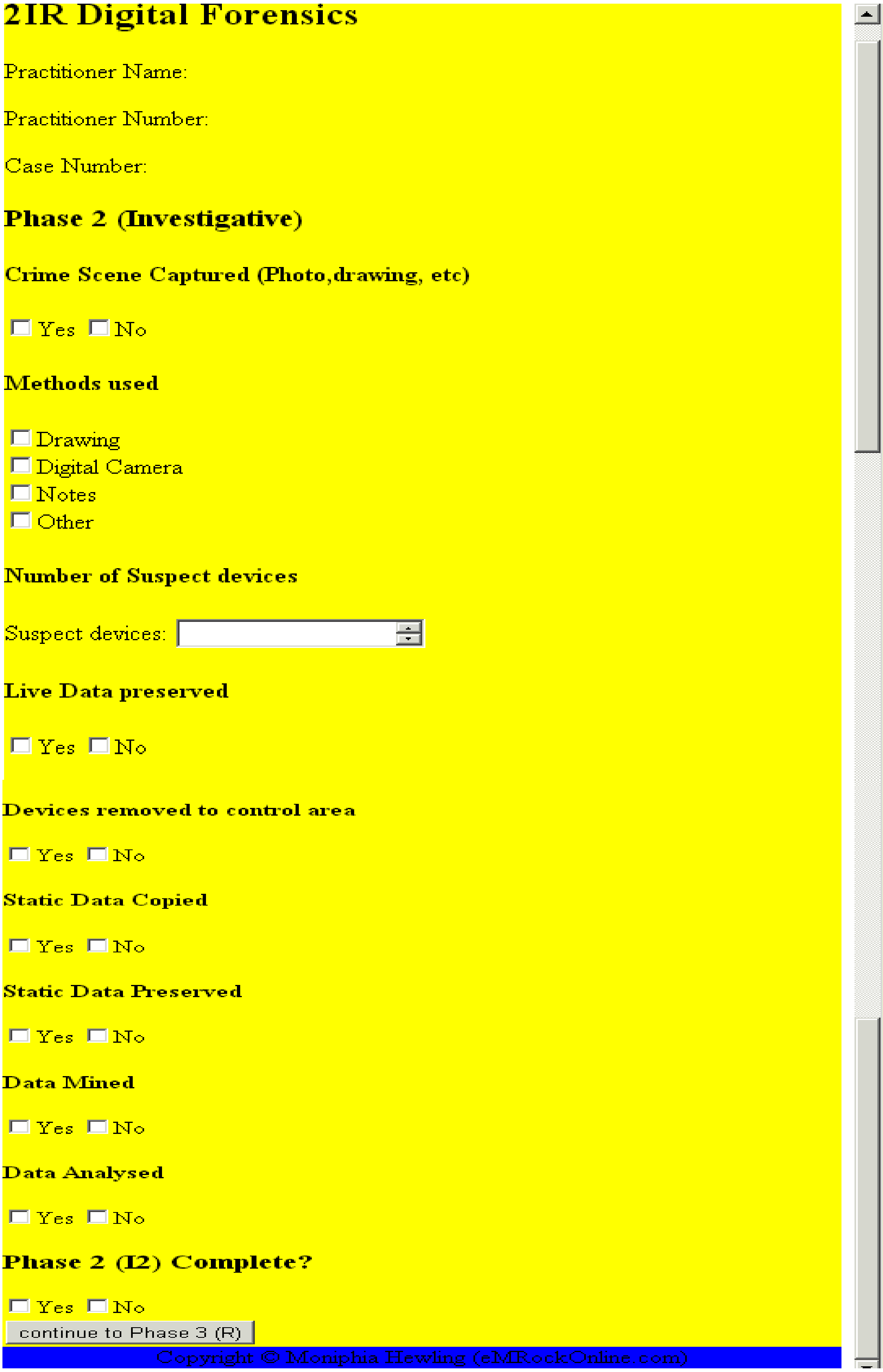
□ Yes, Continue to phase 2

□ No Revisit(enter missing task): [ ]

Copyright © Moniphia Hewling (eMRockOnline.com)

The login screen is followed by the first phase of the application with follows the steps of the 2IR Methodology. It guides the practitioner ensuring that critical administrative steps as outlined in the methodology are followed. At this phase particular basic information captured before will be regenerated. The main objective of the initiation phase generally is to set the stage for the rest of the investigation by assessing the situation and collecting relevant data to ensure that the necessary actions are taken and documents produced before actual seizure and investigation begins.

Phase two screen



2IR Digital Forensics

Practitioner Name:

Practitioner Number:

Case Number:

Phase 2 (Investigative)

Crime Scene Captured (Photo,drawing, etc)

□ Yes □ No

Methods used

□ Drawing
□ Digital Camera
□ Notes
□ Other

Number of Suspect devices

Suspect devices:

Live Data preserved

□ Yes □ No

Devices removed to control area

□ Yes □ No

Static Data Copied

□ Yes □ No

Static Data Preserved

□ Yes □ No

Data Mined

□ Yes □ No

Data Analysed

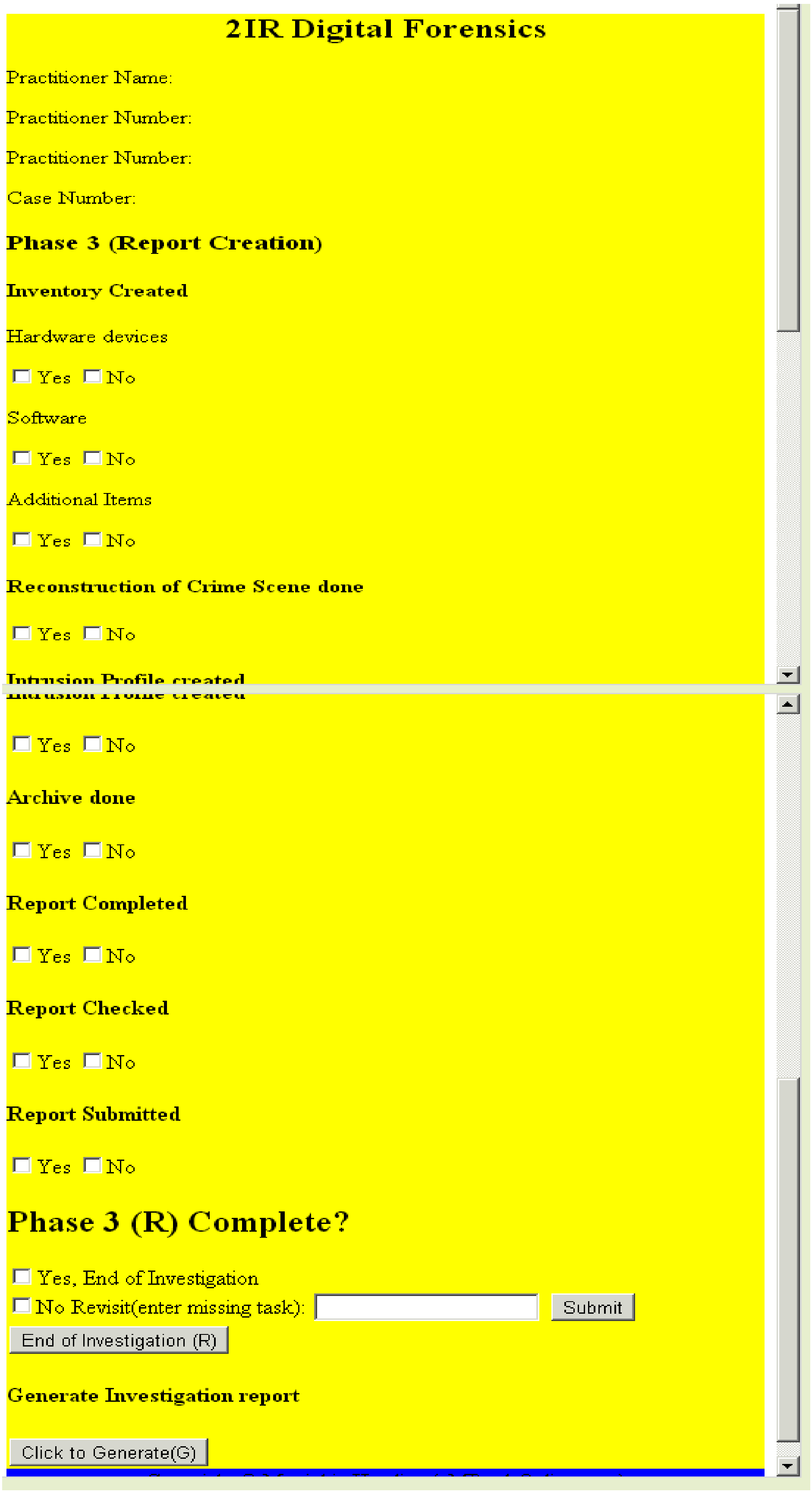
□ Yes □ No

Phase 2 (I2) Complete?

□ Yes □ No

Following completion of the first phase of the Methodology via the Application the second phase then comes onscreen. The Case number, Practitioner's name and number are then reproduced from the previous phases.

Phase three Screen



2IR Digital Forensics

Practitioner Name:

Practitioner Number:

Practitioner Number:

Case Number:

Phase 3 (Report Creation)

Inventory Created

Hardware devices

□ Yes □ No

Software

□ Yes □ No

Additional Items

□ Yes □ No

Reconstruction of Crime Scene done

□ Yes □ No

Intrusion Profile created

□ Yes □ No

Archive done

□ Yes □ No

Report Completed

□ Yes □ No

Report Checked

□ Yes □ No

Report Submitted

□ Yes □ No

Phase 3 (R) Complete?

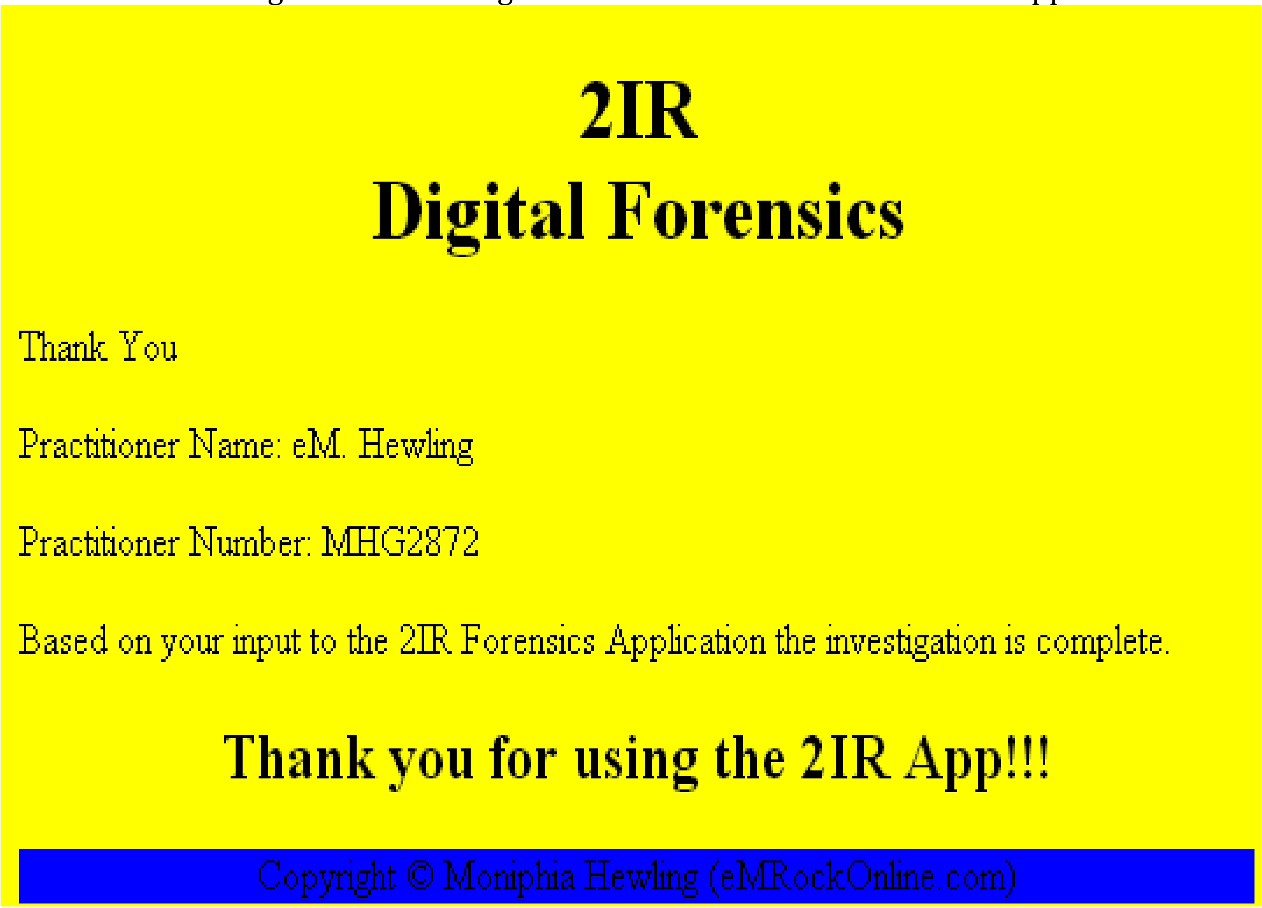
□ Yes, End of Investigation
□ No Revisit(enter missing task): ▭ Submit

End of Investigation (R)

Generate Investigation report

Click to Generate(G)

This is the final section of the application as dictated in the methodology. This phase is totally dependent on completion of the previous phases.
It reproduces data including case number, requesting organisation and practitioners details. Further it accepts the following inputs prompting the user to enter whether or not they have created the necessary inventories as dictated by methodology. Starting immediately after the extraction and analysis of evidence this phase will guide the practitioner in organising the evidence with the first step being to create inventories of all items used throughout the investigation. This will be checked off in the application.



2IR
Digital Forensics

Thank You

Practitioner Name: eM. Hewling

Practitioner Number: MHG2872

Based on your input to the 2IR Forensics Application the investigation is complete.

Thank you for using the 2IR App!!!

Copyright © Moniphia Hewling (eMRockOnline.com)

5.6 Application Review – Discussion of findings

After designing the application the research then continued to ascertain the suitability and relevance of the developed 2IR mobile application to guide the digital forensic process. The interviewees completed and submitted a mini questionnaire with their responses following the interview regarding the other two deliverables (2IR Framework and 2IR Methodology).

Interviewees were asked if they thought the mobile application complemented the 2IR methodology. Twenty three (23) of the thirty (30) respondents said yes it did complement the methodology. Seven of the respondents further suggested that it eliminated the need for

the practitioner to constantly refer to paper based material and travel with bulky documents. Additionally under the choice “other” practitioners responded “Yes but should be further developed”, “No it was the same thing” and “Not sure as I did not get to use it much”.
Eleven(11) of the respondents indicated that they would consider using the application after the testing was completed, eight(8) of this eleven(11) said that this was pending improvements to the current issues they have identified. Two of the practitioners indicated that while they thought a mobile application was a great idea they would not be using such an application in their practice. The remaining eighteen choosing ‘other’ responded with “possibly”,” maybe” and “I would consider it”. These respondents all indicated that with particular improvements to the application they would use it.

With regards to the technical working of the mobile application the research sought to ascertain if the application worked as it was purported to. The objectives of the application included the fact that the application is designed to accept inputs given and produce intermediate output (On screen); The system is easy to use and user friendly. The Inputs will be accepted as indicated and an on screen report produced at the end of the first two phases. The phase screen presented for the phases correspond directly to the phases in the methodology. The application should not allow users to proceed to the next phase unless the current phase completed. If the user does not indicate legal permission to conduct search and seizure the application should produce an error message if they try to continue. The users of the application should also be able to recall already entered data at anytime during the process. Respondents were prompted as to the specific areas that comments were required on. All thirty one of the respondents affirmed that the application did provide guidance through the digital forensics process as dictated by the 2IR methodology. Twenty of the thirty one respondents noted that the application would help in adhering to legal and ethical requirements of the field.

The research then requested general comments from the respondents with regards to the application. Some comments were of a technical nature while others were more general. Twenty Four (24) of the respondents indicated that the application in its current state did not facilitate going back to change data already entered additionally the application would allow them to continue despite any error messages received.

Twenty(20) of the practitioners indicated that the application was a practical idea and that needed to be further developed to eliminate the issues they have encountered. Six(6) of the respondents indicated that the 2IR application was arguably different from other digital forensics application and/or tools they have encountered and that it should be further developed and distributed. One(1) practitioner noted that the colours were inappropriate and should be changed. (The colours are yellow and blue). One(1) practitioner also noted that while this was a great idea it needed to be more secure, being a forensic tool.
Seven of the practitioners/respondents noted that they had issues running the code and suggested that it be properly compiled. The code was written using a combination of HTML5, Java Script and Ajax.   Two(2) practitioners of the group noted that more specific steps similar to those outlined in the 2IR methodology should be included so that both designs totally corresponded.

Eleven of the respondents suggested that a further development of the 2IR mobile application could be the addition of a data mining feature to help in the actual processing of the investigation. One(1) respondent simply replied “great idea but needs more features”.

Summary

The 2IR Application was developed as an accompaniment to the 2IR methodology. The main objective of developing such an application is to alleviate the need for constant referencing to the methodology in print and to eliminate the need for taking around bulky printed material to collect data when in the field. Other objectives included, being available as a guide to ensure maintenance of particular standards and adherence to related laws. These are built into the prompts in the application. There are a number of digital forensics tools available to capture and analyse digital evidence and thus there is very little need for a new tool to perform those functions. Research has revealed however that there is need for standardization in the field and the consideration of facets outside that of technical area. This application was developed with that in mind following the development of the associated 2IR methodology.

CHAPTER SIX

CONCLUSION AND FUTURE WORK

This chapter outlines the findings of the research and is organized as follows; The chapter begins with a look at the concept of cybercrimes, what they are and how they have emerged over the years and a summary of the laws developed in response to them. The chapter continues with the overall conclusion of the study, followed by the impact of this study on the field. The final section will contain recommendations for further research in the field. The chapter then concludes with an overall summary of the research project.

6.1 Rationale

As the increase in the use of digital devices continue and the previously stored analogue data is made digital there is the continued need for digital evidence in cases presented in court. The nature of digital evidence makes it different from other types of evidence presented in court (Casey 2011), (Schatz 2010). It presents issues of being easily changed, easily hidden and changed without the changes being obvious. The process to acquire this evidence is constantly being modified with new models of carrying out the process often being presented. There is currently no existing benchmark model/methodology/framework for practitioners worldwide. This process, digital forensics is still is in its developmental stages as a field and new ways of analysing and interpreting its resultant digital evidence are constantly being developed and formalized. This along with the legal, ethical and investigative aspects of the field need to be versatile enough to adapt to the technological setting in which it is based.

The work presented in this thesis has looked at the field from an integrated perspective, identifying gaps in the field as it relates to standards and procedures required to carry out a digital forensics investigation.

Digital forensics tools, methodologies and laws all work together to make the field viable in tackling the scourge of cyber related criminal activity. To develop a framework and methodology that will effectively tackle the problem of cybercrime there has to be some insight on the activities that are included in cybercrimes and the laws developed to address them. Cyber crime is not consistently defined and its definition varies greatly. Cybercrime is defined as attacks on the cyber security infrastructure of an organization (Gottschalk 2012). This definition may be extended to include country with the recent developments in cyber war. Cyber crime is any criminal activity associated with a computer or related devices. These crimes include new types of criminal activities such as hacking and distributed denial of service as well as traditional crimes being committed or assisted using new technology such as fraud, terrorism, intellectual property infringement and child exploitation. Cybercrimes though they may seem to be outside attacks are at times internal being committed by persons within a company or country. A distributed denial of service attack (ddos) which is the act of overloading a network with requests resulting in either the slowing down of the system or bringing it to a total halt. This act prevents legitimate users from making use of the system during the downtime. The perpetrator does this by engaging the use of multiple computers that have been prepared before hand for such use. There is also hacking which refers to the illegal intrusion or accessing of a computer system and or network. Terrorism (Cyber terrorism), is a term used to describe the use of organized Internet based activities for disruption of services. (Prichard and McDonald 2004) describes cyber terrorism as “politically motivated attacks in cyberspace”. They continue stating that these attacks are intended to cause great harm such as loss of life or severe economic damage. Cyber terrorists use networks as a means of carrying out their destructive activities. Networks facilitate them in a number of ways such as enabling control of a large number of devices and with communication between groups and members.

Intellectual property infringement refers to the infringement of copyright, patent and/or trademark. IP infringement is the use of someone’s intellectual property without permission. The emergence of the internet facilitates this making it easier for people to use other people’s properties without permission seemingly unnoticed. (Gottschalk 2012) notes that, the cyber space provides a conducive environment for software, music and print materials to be downloaded, copied and distributed without permission from copyright owners.

Child exploitation another type of cyber crime has been a plague to the society for some time and the emergence of the internet has not helped in stemming the activity but has facilitated its perpetrators in organizing their activity. (Gottschalk 2012) “identifies online child exploitation to be the use of the Internet to coordinate, lure, persuade, deceive, threaten or coerce children into performing act that are against their rights”. Traditional and online child exploitation may include, child pornography, child labour and child trafficking.

There have been a number of laws enacted by countries internationally to address the increased occurrence cyber/computer related crimes. The nature of cyber/computer related crimes presents the issue of cross border cooperation as the crimes are not necessarily committed in the country where the perpetrator resides. The highlights the need for international cooperation with regard to addressing the issues regarding cybercrime. The ‘Convention on Cybercrime, Budapest 2001 is one such measure that has be undertaken in the past to address these issues. These developments in the field were discussed in chapter 5 Section 2.

Digital forensics has evolved as a discipline to address the increasing issue of computer/cyber related criminal activity.

6.2 The Research and its contributions

The research began with the identification of problematic issues within the field. Following an extensive review of existing literature about the field it was identified that;

- There were a number of issues surrounding the methodologies used in the digital forensics process making the digital evidence less robust in courts. Contribution One (1):
  - The 2IR methodology designed and presented in this research has as its aim to eliminate the existence of such issues. The integrated approach used in creating this methodology and having it governed by a framework of standards helps to ensure that the digital evidence produced is reliable, valid and consistent making it more robust in court.
- There were a number of methodologies existing that are used in the process of acquiring digital evidence. However none of these adequately addresses the core facets of the legal, technical, educational and ethical issues impacting the digital forensics process as a whole. Contribution Two (2):
  - What this research has done is to create a methodology that incorporates all the core facets of the field (legal, ethical, educational, technical) addressing all the related issues identified through an integrated approach.
- There is no existing framework of standards to govern the acquisition of digital evidence. Contribution Three (3):
  - The research output produced in this project has developed an integrated set of standards that will serve as an overarching guide and structure to the digital forensics process and practitioners in the field.
- There is an increase in the use of digital evidence acquired through the digital forensics and electronic discovery in courts worldwide. Contribution four (4)

- The research has produced outputs that will ensure that the digital evidence produced from the digital forensics process are robust and trustworthy when they are put forward to support cases in court.

These issues were further confirmed by the results of a survey undertaken to substantiate the findings found in the literature survey. The research sought answers to the following questions:

- To what extent would a common code of practice for digital forensics practitioners help to bridge the divide in major court cases where the evidence resides in the digital realm?

Extensive analysis of the survey findings as well as the interviews done revealed that the digital forensics field would indeed benefit from the creation of a common code of practice to guide its practitioners. This is mainly due to the fact that digital forensics is the investigative process used to acquire digital evidence from computer/ cyber related criminal activity. These criminal activities at times involve the use of a network and thus may span across national borders and subsequently jurisdictions. Having a common code of practice would help to alleviate jurisdictional and legal issues where this occurs and the cooperation of law enforcement and digital forensics practitioners from across borders is required. This research has put forward such a framework that may be used by practitioners from different jurisdictions to undertake a digital forensics investigation. The 2IR framework of standards is an integrated framework of principles designed to guide the digital forensics field. This framework contains principles and guidelines derived from all the core facets of the digital forensics field namely, legal, technical, education and ethical. It covers the three core phases of the digital forensics investigation (i) Initiation, (ii) investigation and (iii) Reporting.

- How would the development of an integrated methodology governed by a framework of standards in the field allow computer forensics practitioners to capture and preserve digital evidence acquired adequately, keeping in mind the volatility of the data?

An integrated methodology governed by a framework of standards will assist practitioners by providing guidance for the methodology that encapsulates the digital forensic process. A methodology that incorporates all the facets of the digital forensics field and compresses them into one simple methodology means that the digital evidence is acquired in a uniformed fashion that supports all the legal, technical and ethical issues to be observed.

Such a methodology, in dictating how to do what is to be done ensures compliancy without any additional effort on the part of the practitioner. The methodology proposed in this research has employed an integrated approach incorporating the core facets of the digital forensics field facilitating a simplified precise methodology that may be employed by practitioners from varying backgrounds and jurisdiction.

- Would a methodology facilitating accurate and timely tracking and identification of individuals involved in a digital crime address the problems currently encountered by practitioners in the field with regards to the promotion of digital evidence in courts of law?

A methodology that facilitates the accurate and timely tracking and identification of individuals alleged to be involved in a computer related crime would be of benefit to the field. Other forensics fields have as their core the objective of identifying what happened where and by whom. The inclusion of steps such as reconstruction of the incident and the creation of an intruder profile readily facilitates the tracing of the incident with regards to time and person/s involved. The inclusion of these two critical components in one methodology that is governed by a framework of standards is an improvement to the field. The 2IR Methodology produced by this research integrates the core elements of a forensics investigation producing a methodology that will produce evidence that conforms to the standards of a court of law. It details the tasks to be performed in a digital forensics investigation under three phases, (i) initiation, (ii) investigation and (iii) reporting. It is designed to be prescriptive while improving accuracy in how the process is carried out and to produce digital evidence that meets the criteria for being acceptable in court.

- Would a framework of standards governing how the acquisition of digital evidence is carried out help to make digital evidence more robust in court?

Results analyzed from the testing of the framework of standards revealed that practitioners conclude that having a framework of standards that govern how the digital evidence is acquired would definitely help to make the digital evidence acquired more robust in court. This research produces a framework of standards (2IR Framework of standards) governing the field of digital forensics and more specifically the 2IR Methodology. In recognition of this deficit in the field the creation of the 2IR framework of standards is a timely response to a specific need in the digital forensics field. These developed standards can be used across jurisdictions and offer a way to ensure reliability and trustworthiness in the digital evidence retrieved from the digital forensics process.

In a technologically driven society all institutions whether it is their core field or not, use information. This information has become a valuable commodity and thus is usually protected for threats both inside and out of the organization. The importance of the commodity information, is also highly sought and often under threat by both insiders and outsiders resulting in attacks of various types. For this reason there has had to be an active effort on the part of organizations, law enforcement and even governments to put measures in place not only to stem, but to investigate occurrence of cyber/computer related criminal activity.

Careful analysis of several cases that involved the use of digital evidence acquired through the digital forensics process suggests that though significant strides have been made in the area more needs to be done. Research has revealed that there is evidence in the results of several court cases that practitioners in the field need a standardized set of procedures with which to operate.

The 2IR framework of standards is an integrated framework of principles designed to guide the digital forensics field and specifically the 2IR methodology. It dictates standards from all the core facets of the digital forensics field and covers the three main phases in any digital forensics process, (i) initiation, (ii) investigation and (iii) reporting. The derived 2IR Methodology presented in this research integrates the core elements of a forensics investigation producing a methodology that will produce evidence that conforms to the standards of a court of law. It dictates the tasks to be performed in any digital forensics investigation (cloud, mobile, computer etc). These tasks fall into one of the three phases, (i) initiation, (ii) investigation and (iii) reporting. Additionally the 2IR methodology includes two very critical components of the forensics process, reconstruction of the crime scene and suspect profiling. It is designed to be prescriptive while improving accuracy in how the process is carried out and aims to produce digital evidence that meets the criteria for being acceptable in court

Some additional specific observations from this research include;

1. Digital forensic practitioners are now in demand and will continue to be for the foreseeable future.
    a. The research revealed that digital evidence is increasingly becoming a part of cases being presented in courts. This type of evidence is becoming predominant in both civil litigations as well as criminal cases involving

traditional criminal activities and technologically related crimes. This has resulted in the need for strict rules and guidelines regarding the process of digital forensics, the process used to acquired digital evidence as well as trained professionals to perform the duty.

2. Digital evidence can prove useful in court to enable the conviction or acquittal of an accused if properly acquired, preserved and presented. A case may have a negative result if the digital evidence related to the case is not properly handled. Examples outlined in the cases in Chapter 5 Section 2.
    a. Reliability and consistency are some of the issues identified with digital evidence when presented in courts. The 2IR designs presented in this research incorporates proven techniques used in forensics science traditionally to ensure that the evidence produced not only meets the criteria for acceptability in courts but is able to withstand the rigours of a courtroom.
3. Computers are involved in a number of traditional criminal activities thus digital/computer forensics is now more popular as a part of non-computer based crimes, a point supported by (Kessler 2010) and (Mason 2013) as well as civil investigations.
    a. The increased acceptance and use of technological devices in all aspects of life worldwide has prompted the increase in these devices being used in the committing of traditional crimes or being involved in some way with crimes such as drug trafficking and accounting fraud. These occurrences highlight the need for a structured process to apprehend the perpetrators of these crimes.
4. Digital forensic practitioners are often required to present and explain their finding in court thus performing the role of an expert witness. Points supported by (Mason 2013).
    a. Digital forensics like other forensics sciences requires that their practitioners be knowledgeable of their field enough to be able to present their findings to persons from varying backgrounds. The role of an expert witness is critical in the presentation of evidence which helps to its validity and reliability. This indicates the importance of properly trained practitioners in the field as well as proper documentation of the process.
5. As the use of digital evidence in courts increase, there is the increased need for the use of trained practitioners who perform or participate in the digital forensics process. Points supported by (Mason 2013)

a. The current state of digital forensics is one that is gradually developing but still somewhat disjointed and ad hoc with no international body or set of standards being one of the main issues. The current challenges faced by information security personnel will not disappear anytime soon and thus the training of digital forensics professional is in demand. Commercial companies that manufacture tools for digital forensics investigations are the major playing in training practitioners for the field (eg. Guidance Software and SANs Forensics) providing individual professional qualifications for their tools. While this is important there must be some collaboration with these companies and academics to ensure that the field is uniformly developed. This research highlighted one aspect of the field that needs to be improved for the field to be regarded and a true forensics science and help to improve the robustness of the evidence produced from the digital forensics process. Having a standardized education programme such as the one presented by this research producing well rounded practitioners in the field will eradicate some of the current issues existing in the field. The 2IR curriculum designed for the training and education of digital forensics practitioners is developed to ensure that with proper execution practitioners possessing the qualities desired by the field are produced.

The dynamic nature of technology combined with the increase in its use by members of society has resulted in the increased need for forensic investigators and their services. Digital crimes are becoming more complex as technology develops thus practitioners, their methodology and the tools they employ must be able to keep abreast with the criminal minds. Currently there is no one distinct methodology incorporating all elements of digital forensics in place that is used as a standard for the field. Digital evidence has become increasingly popular and courts have had to deal with an increase of cases that involve the use of digital evidence in recent times. The procedures currently used in the digital forensic process to acquire this evidence were developed focusing on particular areas of the acquisition process depending on the developer's expertise or interest. The 2IR methodology presented in this research is integrated and does not focus on any particular facet or phase but focuses on the digital forensics process as a whole. This positions the 2IR methodology to be dynamic and flexible enough to be used as a standard benchmark by practitioners from different jurisdictions.

This research highlighted a number of issues surrounding the process of acquiring digital evidence which is the digital forensics process. The 2IR framework, methodology, application and curriculum are designed to address these issues.

With the already high and increasing prevalence of computer related crimes such a framework is needed to ensure that the field not only grows but remains viable as continued research is carried out facilitating improvement. In developing the deliverables of this project a number of factors were taken into consideration. These included the different fields that would contribute to the growth and development of digital forensics as a true forensics science discipline. These fields were legal, Computer Science (technical), education including information security and ethics as it relates to investigation and evidence.

6.3 Transferability and future work.

The 2IR framework of standards may be used as a basis for developing ISO standards specific to the digital forensics process.

The work done in this research may be used by academics to further develop academic and /or training programmes in the field of digital forensics.

The application developed as an accompaniment to the 2IR methodology can be further developed to include data mining and/or analysis features.

The developed curriculum can be used in training and educational programmes for law enforcement and other related personnel wishing to embark on such programmes.

It is hoped that the findings of this research will influence academics and practitioners to ensure that all facets of the digital forensics field are integrated in their practice. That this project has highlighted the need for an integrated approach to the practice of digital forensics to ensure the acceptability of the digital evidence acquired.

6.4 Direct Contribution to the digital forensics field

1. The 2IR Framework of standards is the first such framework of standards created for the field of digital forensics. (novelty)
2. The 2IR methodology is not just another methodology but one that includes all the critical aspects of a digital forensics investigation. For example, legal adherence incorporated, reconstruction of the incident scene, intruder profiling and ethical adherence. (contribution)
3. The 2IR methodology is derived from and works in conjunction with a developed framework of standards based on legal, technical, ethical and educational principles. (contribution)
4. An application simplifying the methodology for ease of use and mobility. (contribution)

The 2IR package includes element critical to the development of the field as true forensic science discipline.

- A set of standards incorporating all four core facets (technical, legal, educational, and ethical) of the digital forensics field.
- A mobile application based on similar principles to the developed 2IR methodology guide the practitioner through the process.
- A curriculum of studies to ensure the preparedness of practitioners function effectively in field all throughout the process to being an expert witness.

This work is a substantial addition to the established methods/ methodologies for acquiring digitally stored data/information for use in a court of law. It adds to the knowledgebase an integrated and exhaustive set of standards that did not exist before in the field. There is also the addition of an integrated methodology for acquiring digital evidence that also exists electronically. This methodology guides practitioners through the process ensuring adherence to legal and ethical standards of performance.

Summary

This research is a substantial addition to the already established methods/methodologies designed for the acquisition of digitally stored data to be used as evidence in a court of law. It adds to the academic knowledgebase as well as the practical area of performing a digital forensics investigation. This research presents a set of standards that do not currently exist within the field of digital forensics. These standards are exhaustive integrating the four core facets of the digital forensics field and addressing the three main phases of a digital forensics investigation.

The deliverables are as a result of in dept investigation into the current state of the digital forensics field with regards to the policies, guidelines and methodologies/models used throughout the digital forensics process. The research looks specifically at these with a focus on the legal, ethical educational and to a lesser extent the technical facets of the field.

APPENDICES

Appendix A - The 2IR framework of Standards

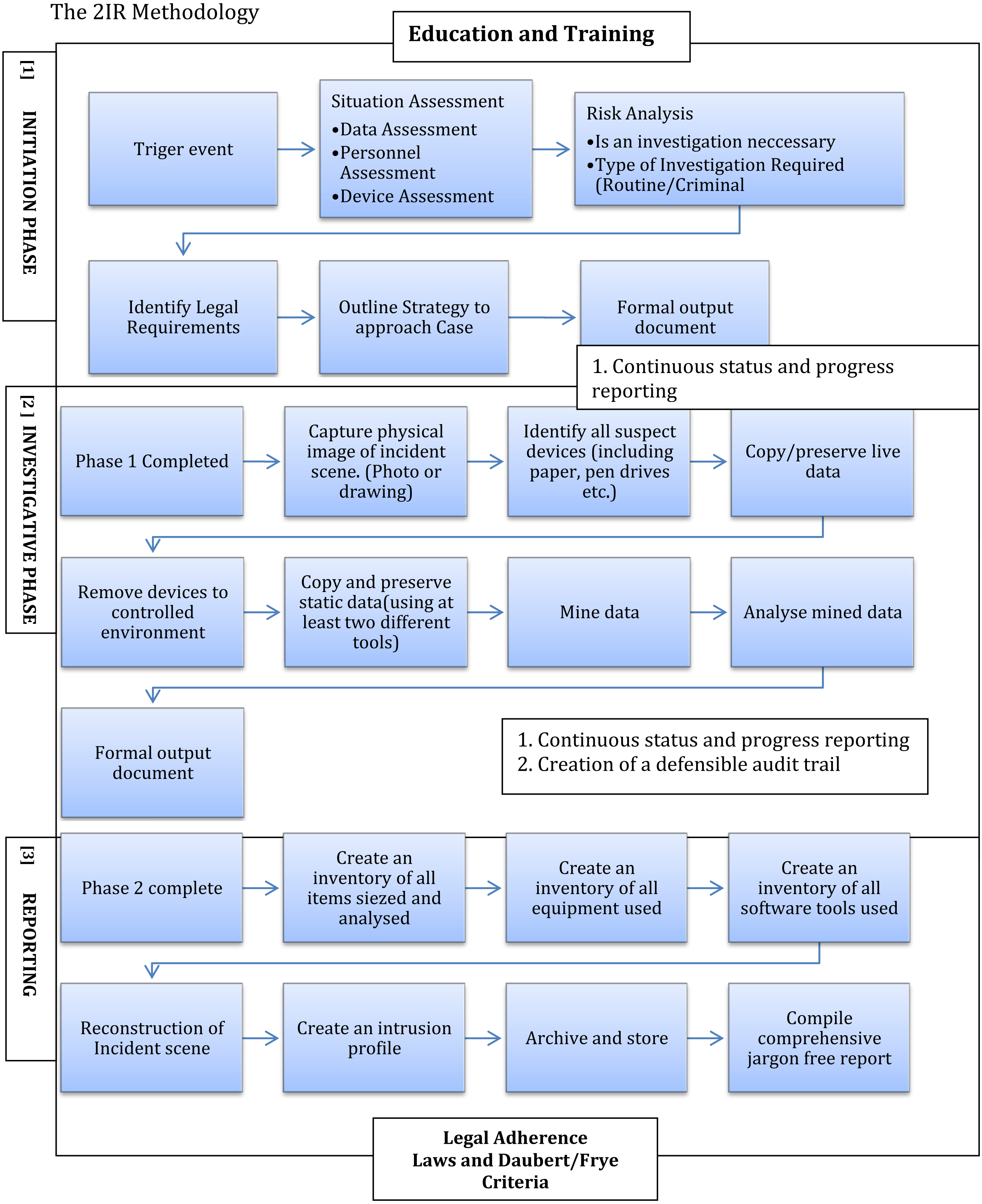
FRAMEWORK	Technical (T)	Legal (L)	Educational (E)	Ethical (E_1)
Core Principles: **C1. Practitioners should be knowledgeable of the current legal requirements and policies impacting the investigation. [L/Ed]** **C2. Practitioners should be trained and qualified in the area of digital forensics and handling digital evidence. [Ed]** **C3. Two or more tools should be used in an investigation ensure accuracy of the results. [T/Ed]** **C4. Practitioners should keep up to date with the developments in the field through training, workshops. Conferences and research publications. They should evaluate their performance regularly and be committed to improving their practice through professional development and training. [E]** **C5. Practitioners should have positive values and attitudes and adopt high standards of integrity in their professional role. [Ed]** **C6. Practitioners should be familiar with a variety of operating systems. [T]**	T1 Have grounded knowledge and experience in using at least two commercial digital forensics tools (not open sourced) to extract data. T2. Be aware of the limitations of the various digital forensics tools and strategies to overcome them. T3. Have sufficient depth of knowledge about the tools they use to be able to become expert witness T4. Know how to identify and address problems with tools and/or equipment that they use and when to refer them.	L1 Be aware of the current legal requirements, national/international policies and guidance regarding capturing digital evidence. L2. Be aware of the legal documents required for use before, during and after the digital forensics process. L3. Create and maintain an audit trail in accordance with the law. L4. Know the different laws applicable to a digital forensic investigation.	E1. Have secure knowledge and understanding of the legal context in which they will function E2. Know and understand the techniques used in a digital forensics examination. E3. Know, understand and respect the roles of self, colleagues and other stakeholders E4. Have sufficient knowledge to be able to give advice on the different stages of a digital forensic investigation as well as different tools used. E5. Knowledgeable on investigative techniques used in the field.	$E_1$1. Observe local and international policies and guidelines when doing a digital forensic examination. $E_1$2. Know how to effectively communicate with teams members and observe the chain of command. $E_1$3. Know when to draw on the knowledge and experience of colleagues. $E_1$4. Ensure transparency throughout the investigation.

	Tools and Procedures	***Procedures***	***Certifications and qualifications***	***Roles and responsibilities***
Initiation **(I_1)** $I_1$1. Practitioners must observe the legal requirements for the authorization and capture of digital evidence. $I_1$2. Practitioners must be cognizant of the expectations of all stakeholders.	$TI_1^{(1)}$ Know the range of devices that may be involved in the investigation. $TI_1^{(2)}$ Select appropriate tools based the digital devices to be encountered in the investigation.	$LI_1^{(1)}$Aware of legal requirements for the capturing of digital evidence. $LI_1^{(2)}$ Select tools for the investigation in accordance with the recommended principles and guidelines.	$EI_1^{(1)}$Posses the educational background and capability to handle all aspects of the investigation. $EI_1^{(2)}$ Select tools that the practitioner has been trained to use.	$E_1I_1^{(1)}$Disclose any conflict of interest with regards to the impending investigation. $E_1I_1^{(2)}$Approach the investigation objectively.
Investigation **(I_2)** $I_2$1. Practitioners must adhere to guidelines to ensure sound retrieval of digital evidence. $I_2$2. Practitioners must observe techniques to ensure preservation of digital evidence before, during and following acquisition. $I_2$3. Practitioners must ensure correct measures are taken to protect the scene of the incident.	$TI_2^{(1)}$Appropriate methods and techniques are used in accordance with the recommended guidelines. $TI_2^{(2)}$Ensure tools used are clearly understood and can be used by another investigator and produce the same results	$LI_2^{(1)}$Ensure that methods used can be reproduced by other investigators producing the same results. $LI_2^{(2)}$ Be aware of the laws associated with the investigation at this stage. $EI_2^{(3)}$Treat all data and devices as potential legal evidence.	$EI_2^{(1)}$Ensure that practitioner is trained to use the tools available where open source or commercial. $EI_2^{(2)}$Ensure knowledge of the different tools to be used for different purposes throughout the examination. $EI_2^{(3)}$Treat all data and devices as potential legal evidence. $EI_2^{(4)}$ Be Knowledgeable of the tools they work with and how they do what they do.	$E_1I_2^{(1)}$Maintain objectivity throughout the investigation $E_1I_2^{(2)}$Treat all data and devices as potential legal evidence. $E_1I_2^{(3)}$Exercise care to ensure to ensure the integrity of the evidence acquired. $E_1I_2^4$ Ensure validity and reliability in the materials analyzed.
Report **(R)** *R1.* Practitioners should ensure accuracy in classifying and reconstructing the incident scene. R2. Practitioners should be constructive in producing a relevant report. R3. Practitioners should recognize that this phase may include being an expert witness. R4. Practitioners should be reflective and responsible for identifying drawbacks and facilitate ways for improvement.	TR^1 Archive all software tools used. TR^2 Archive all hardware tools used	LR^1 Document all hardware tools used in accordance with the recommended guidelines. LR^2 Document all tools in accordance with the recommended guidelines LR3 Regardless of legal definitions, a digital forensics practitioner will realize that there are degrees of certainty represented under the single term of expert opinion. The practitioner will not take advantage of the general privilege to assign greater significance to an interpretation than is justified by the available data.	ER^1 Practitioners must have sound knowledge in the reconstruction of a digital crime scene. ER^2 Practitioners must be knowledgeable in archiving and documenting tools used ER^3 Practitioners must adequately trained to produce a comprehensive report of the investigation. ER^4 Posses training to interpret findings accurately ER^5 Be knowledgeable in creating an attacker profile.	$E_1R^{(1)}$ Practitioners must ensure confidentiality in the findings of the investigation. $E_1R^{(2)}$ Practitioners must ensure full disclosure of their findings to the relevant personnel. E_1R_3 When a practitioner works as an expert witness they will not take advantage of the privilege to express opinions by offering opinions on matters within their field that is not necessarily their area of expertise.

				E_1R_3 Conclusions should not be drawn from materials that atypical and/or unreliable. E_1R_4 Where results are inconclusive or indefinite any conclusions drawn should be fully explained in the report.

.

Appendix B
The 2IR Methodology


Education and Training
[1] INITIATION PHASE
Triger event
Situation Assessment
•Data Assessment
•Personnel Assessment
•Device Assessment
Risk Analysis
•Is an investigation neccessary
•Type of Investigation Required (Routine/Criminal
Identify Legal Requirements
Outline Strategy to approach Case
Formal output document
1. Continuous status and progress reporting
[2] INVESTIGATIVE PHASE
Phase 1 Completed
Capture physical image of incident scene. (Photo or drawing)
Identify all suspect devices (including paper, pen drives etc.)
Copy/preserve live data
Remove devices to controlled environment
Copy and preserve static data(using at least two different tools)
Mine data
Analyse mined data
Formal output document
1. Continuous status and progress reporting
2. Creation of a defensible audit trail
[3] REPORTING
Phase 2 complete
Create an inventory of all items siezed and analysed
Create an inventory of all equipment used
Create an inventory of all software tools used
Reconstruction of Incident scene
Create an intrusion profile
Archive and store
Compile comprehensive jargon free report
Legal Adherence
Laws and Daubert/Frye Criteria

Appendix C
Sample Forms

Data Assessment Form *DA1*

CASE #:

LEAD PRACTITIONER NAME:

PRACTITIONER NUMBER:

DATE:

TYPE OF DATA:		FINANCIAL PERSONAL GENERIC
STATUS OF DATA		ENCRYPTED PASSWORD PROTECTED OPEN
TYPE OF DATA MANAGMENT SYSTEM		CENTRAL DISTRIBUTED OUTSOURCED (Cloud etc.)
DATA BACKED UP	YES	NO

Practitioner Name:..

Practitioner Signature:.......................................

Date:................................

Special Comments:...

Device Assessment Form DA2

CASE #:

LEAD PRACTITIONER NAME:

PRACTITIONER NUMBER:

DATE:

Types and Number of Devices

Types	Number	Comments
Workstations		
Laptops		
Notebooks		
Macbooks		
Memory Stcks		
Mobile Devices:		
Tablets		
Phones		
PDAs		
Others		

Practitioner Name:..

Practitioner Signature:.......................................

Date:................................

Special Comments:...

Initial Assessment Form IAF

To be completed on initially meeting the client

Case#:

Case Name#:

Responder:

Date:

INTENT OF INVESTIGATION

SCOPE OF INVESTIGATION

IS THERE AN INTERNAL INCIDENT REPONSE TEAM/PERSON/POLICY

WHO DISCOVERED THE INCIDENT
WHAT WAS REPORTED

WHAT TYPE OF DATA IS THREATENED

WHAT CONSTITUTES THE ATTACK (eg. DDOS, Virus etc)

LEGAL RESTRICTIONS

LIMITATIONS OF INVESTIGATORS AUTHORITY

Intrusion Assessment Form IAF

CASE #:

LEAD PRACTITIONER NAME:

PRACTITIONER NUMBER:

DATE:

SUSPECTS: □ Known □ Unknown
NUMBER OF SUSPECTS

ORIGIN OF INTRUSION □ Internal □ External

POSSIBLE MOTIVES

WHO KNOWS OF THE INCIDENT

CIRCUMSTANCES

WAS/IS THERE AN INTERNAL TEAM ASSIGNED TO THE CASE

Practitioner Name:..

Practitioner Signature:.......................................

Date:................................

Special Comments:..

Personnel Assessment Form DA2

CASE #:

LEAD PRACTITIONER NAME:

PRACTITIONER NUMBER:

DATE:

Item	**Available**	**Not Available**	**Outsourced**	**Comments**
Skills Required				
Hardware Tools Required				
Software Tools Available				
Cost-Who will fund investigation	Practitioner	Requesting Company	N/A	
Time – Can it be completed in the time required	Yes	No	Time	
Suitable qualifications			Outsourced	

REQUESTER RISK ASSESSMENT (CRA)

	Yes	No	Comments
Downtime Allowed			
Investigation – Value Added			
Repercussion of exposure	Level (highest) 1 2 3 4 5 (Lowest)		

Practitioner Name:..

Practitioner Signature:.......................................

Date:.................................

Special Comments:..

System/s Assessment Form SA1

CASE #:

LEAD PRACTITIONER NAME:

PRACTITIONER NUMBER:

DATE:

Operating System/s	Hardware Platform/s
1.....................................	1.....................................
2.....................................	2.....................................
Number of Systems	Hard Drive/s
	Number
	Type/s
Other Locations	Remote
Server/s(Location/type)	

Documents Collected	**Yes**	**No**	**Comments**
Systems List			
Development Plans			
Maps/Diagrams			
Flowcharts/Data Flow Diagrams			
Schedules			
Organisational Charts			

Practitioner Name:...

Practitioner Signature:.......................................

Date:................................

Special Comments:..

Suggested Initial Interview questions

CASE #:

INTERVIEWING PRACTITIONER:

PRACTITIONER NUMBER:

DATE:

After responding to the incident and an interview is arranged these are some data that the investigating team will need to gather.

1. Ascertain exactly what the client requires from the investigation

   a. What does the client wish to achieve from the investigation?

   b. What is the objective of the investigation? (file criminal charges, policy abuses etc)

2. What are the companies policies regarding the incident?

   a. What are the legal procedures for the company re incidents of that nature.

   b. Does the company have a legal officer?

3. What is the scope of the investigators/investigating teams authority?

   a. Will someone from the organisation be assigned to the team?

   b. What authority doe the investigator/investigating team have?

   c. What are the escalation procedures?

4. What are the fact regarding the incident?

   a. Who discovered the incident?

   b. Who reported the incident?

   c. What is it that is alleged to have happened?

   d. Who are the people who know of the incident?

NB. The investigator needs to ascertain if the will be able to interview individuals if the investigations require them to.

Appendix D
Application Codes

Landing Page

```
<!DOCTYPE html>
<html>
<body>
<div id="container" style="width:500px">
<div id="header" style="background-color:#0000FF;">
<h1 style="margin-bottom:0;">The 2IR Methdology</h1></div>
<div id="header" style="background-color:#FFFF00;">
<h3 style="margin-bottom:0;">Facets:     Technical(T) Legal(L)  Education (E)Ethical (E1)</h3></div>
<div id="menu" style="background-color:#FFFF00;height:200px;width:100px;float:left;">
<b>Phases</b><br>
Initiation (I1)<br>
Investigative (I2)<br>
Reporting (R)</div>
<div id="content" style="background-color:#00FF00;height:200px;width:400px;float:left;">
The 2IR methodology has three major phases ( described in the framework) that will be further broken down in to more specific steps.  It is designed to be prescriptive and rigorous while ensuring speed and accuracy.  It is prescriptive because it will include recommendations of the use of particular tools at different stages in the process and is guided by standards.  It is rigorous because it is expected that no phase will be excluded.  This measure ensures the model is accurate and reliable.  Educational training and qualification along with legal and ethical principles encompass the methodology.</div>

<div id="footer" style="background-color:#0000ff;clear:both;text-align:center;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>

</div>
```

```
</body>
</html>
```

Idle page

Login Page

```
<htm4>
<body>

<h1>2IR Digital Forensics </h1>
<body style="background-color:yellow;">

<form>
Practitioner Name: <input type="text" name="firstname"><input type="text"
name="lastname"><br>
PractitionerNumber<input type="number" number="PractitionerNumber">
<br>

</form>

<form action="demo_form.asp">
 Date (date and time): <input type="datetime" name="daytime">

</form>

<form name="input" action="html_form_action.asp" method="get">
UserID: <input type="text" name="user">

Password: <input type="password" name="pwd">
<input type="submit" value="Submit">
</form>
```

```
<br>
<br>
<br>
<div id="footer" style="background-color:#0000ff;clear:both;text-align:left;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>

</div>

</body>
</html>
```

Case detail Page (Page 3Coding)

```
<htm2>
<body>
<div id="header" style="background-color:#FFFF00;">
<h2><center>2IR Digital Forensics</center></h2>

<p><b>Practitioner Name:    </b></p>
<p>Practitioner Number:   </p>

<form>
Requesting Organisation: <input type="text" Requester="Requester"><br>
Contact Name: <input type ="text" ContactName="ContactName"><br>

Type of Organisation: <input type="text" requester="requestingOrganisation"><br>
Location/s: <input type ="text" Location="Location"><br>
Date of Request: <input type= "date" Date of Request="date"><br>

<h4>Nature of investigation Requested</h4>
Criminal <input type="text" name="Criminal"><br>
Routine/Civil/eDiscovery: <input type="text" name="non criminal">

<h4>Investigation required</h4> <br>
```

```
<input type="checkbox" name="Yes" value="Yes">Investigation required<br>
<input type="checkbox" name="No" value="No">No Investigation Required
</form>

<h4>Legal Authorisation needed</h4>
<input type="radio" name="internal" value="internal">internal<br>
<input type="radio" name="External" value="external">external
<form/>
</body>
<body>
<input type="button" onclick="myFunction()" value="Continue to phase one (I1)" />
<div id="footer" style="background-color:#0000ff;clear:both;text-align:center;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>
</div>
</body>

</htm2>
```

Phase 1 The Initiation Phase

```
<htm5>
<body style="background-color: yellow;">
<h1>2IR Digital Forensics</h1>
<p>Practitioner Name:     </p>
<p>Practitioner Number:   </p>
<p>Case Number:  </p>
<form>
<h3>Phase 1 - Investigative (I1) </h3>
<h4> Assessments complete?</h4>
<p>Data Assessment</p>
<input type="checkbox" name="answer" value="Yes">Yes
```

```
<input type="checkbox" name="answer" value="no">No
<p>Pesonnel Assessment</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<p>Device Assessment</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Risk analysis complete?</h4>
<p>General Risk Analysis</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<p>Personal/Practitioner Risk Analysis</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<p>Requester/Company Risk Analysis</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Legal permission been acquired?</h4>
<p>legal Authorisation</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<p>Type</p>
<input type="checkbox" name="answer" value="Yes">Warrant
<input type="checkbox" name="answer" value="no">Permission<br>
<p><b> NB. all analysis and assessments must be complete before the investigation
continues.  It is recommended that legal advice and authorisation be received before
any further are steps taken. </b> <br><br>
<h2>Phase 1 (I1) Complete?</h2>
<input type="checkbox" name="answer" value="Yes">Yes, Continue to phase 2 <br>
<input type="checkbox" name="answer" value="no">No Revisit(enter missing task):
<input type="text" name="user">
<input type="submit" value="Submit">
</form>
```

```
<head>
<script>
function myFunction()
{
alert("Do you want to continue!");
}
</script>
</head>
<body>
<input type="button" onclick="myFunction()" value="Continue to phase two (I2)" />
<div id="footer" style="background-color:#0000ff;clear:both;text-align:center;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>
</div>
</body>
</htm5>
```

Phase 2 Investigative phase

```
<!DOCTYPE html>
<div id="header" style="background-color:#FFFF00;">
<h2>2IR Digital Forensics</h2>
<p>Practitioner Name:  </p>
<p>Practitioner Number:  </p>
<p>Case Number: </p>
</form>
<h3>Phase 2 (Investigative) </h2>
<h4>Crime Scene Captured (Photo,drawing, etc)</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<br>
<h4>Methods used</h4>
<form>
<input type="checkbox" name="capture" value="Drawing">Drawing<br>
```

```
<input type="checkbox" name="capture" value="Digital Camera">Digital Camera<br>
<input type="checkbox" name="capture" value="Notes">Notes<br>
<input type="checkbox" name="capture" value="Other">Other
</form>
<h4>Number of Suspect devices </h4>
<form>
Suspect devices: <input type="number" name="suspectdevice/s"><br>
<h4>Live Data captured</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Devices removed to control area </h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Static Data Captured </h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Data Mined </h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Live data preserved </h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Static data preserved </h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4> Data Analysed </h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<h4>Tools used </h4>
<form>
Software Tools: <input type="text" name="firstname">
<input type="text" name="firstname"><br>
Hardware Tools: <input type="text" name="lastname">
```

```
<input type="text" name="firstname"><br>
</form>
<h3> Phase 2 (I2) Complete? </h3>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No<br>
<form/>
<head>
<script>
function myFunction()
{
alert("Do you want to continue!");
}
</script>
</head>
<body>
<input type="button" onclick="myFunction()" value="continue to Phase 3 (R)" />
</body>
<div id="footer" style="background-color:#0000ff;clear:both;text-align:center;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>
</div>
```

Phase 3 Reporting

```
<!DOCTYPE html>
<div id="header" style="background-color:#FFFF00;">
<h2><center>2IR Digital Forensics</center></h2>
<p>Practitioner Name:     </p>
<p>Practitioner Number:   </p>
<p>Practitioner Number:  </p>
<p>Case Number: </p>
<h3>Phase 3 (Report Creation) </h3>
<form>
<h4>Inventory Created</h4>
```

```
<p>Hardware devices</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<p>Software</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<p>Additional Items</p>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No

<h4>Reconstruction of Crime Scene done</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No

<h4>Intrusion Profile created</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<h4>Archive done</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<h4>Report Completed</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<h4>Report Checked</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
<h4>Report Submitted</h4>
<input type="checkbox" name="answer" value="Yes">Yes
<input type="checkbox" name="answer" value="no">No
</form>
<h2>Phase 3 (R) Complete?</h2>
<input type="checkbox" name="answer" value="Yes">Yes, End of Investigation <br>
```

```
<input type="checkbox" name="answer" value="no">No Revisit(enter missing task):
<input type="text" name="user">
<input type="submit" value="Submit">
</form>
<head>
<script>

<head>
<script>
function myFunction()
{
alert("Do you want to continue!");
}
</script>
</head>
<body>

<input type="button" onclick="myFunction()" value="End of Investigation (R)" />
<h4>Generate Investigation report</h4>
<input type="button" onclick="myFunction()" value="Click to Generate(G)" />
</body>
<div id="footer" style="background-color:#0000ff;clear:both;text-align:center;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>
```

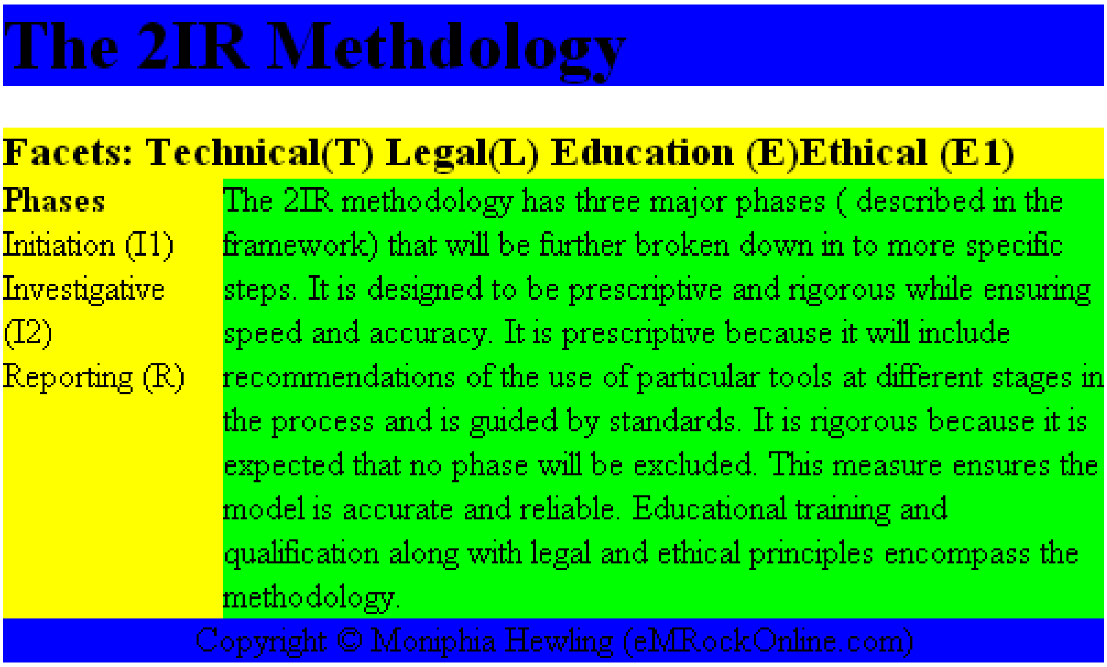
End of investigation

```
<!DOCTYPE html>
```

```
<html>
<body>
<body style="background-color:yellow;">
<h1><center>2IR <center>Digital Forensics </center></h1>
<p>Thank You
<p>Practitioner Name:     </p>
<p>Practitioner Number:   </p>
<p>Based on your input to the 2IR Forensics Application the investigation is complete.
</p>


<h2><center>Thank you for using the 2IR App!!!</center></h2>

</body>
</html>
<div id="footer" style="background-color:#0000ff;clear:both;text-align:center;">
Copyright © Moniphia Hewling (eMRockOnline.com)</div>

</div>
```

Appendix E
Screenshots of Application

Landing Page



The 2IR Methdology

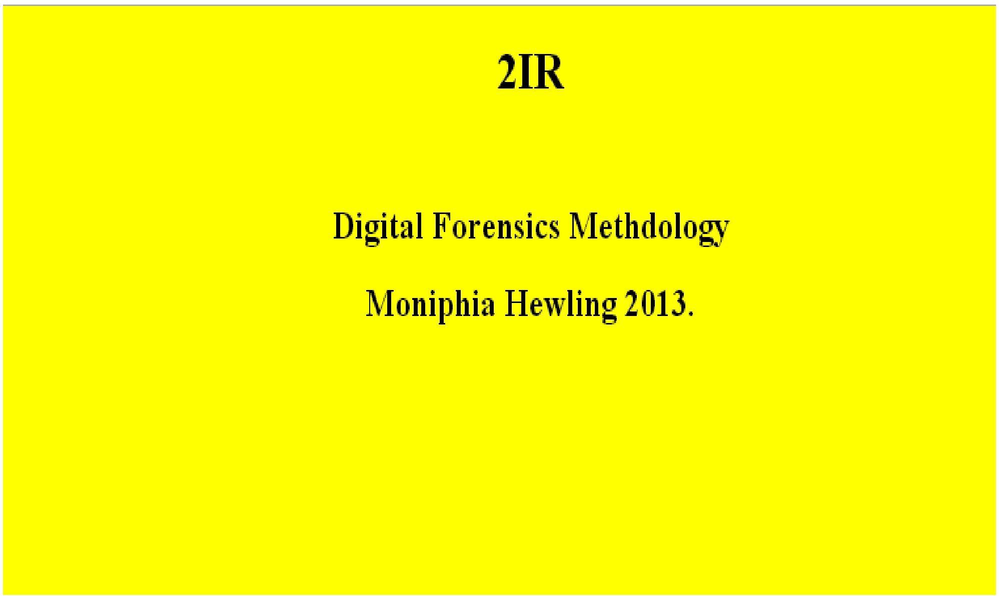
Facets: Technical(T) Legal(L) Education (E)Ethical (E1)

Phases
Initiation (I1)
Investigative (I2)
Reporting (R)

The 2IR methodology has three major phases (described in the framework) that will be further broken down in to more specific steps. It is designed to be prescriptive and rigorous while ensuring speed and accuracy. It is prescriptive because it will include recommendations of the use of particular tools at different stages in the process and is guided by standards. It is rigorous because it is expected that no phase will be excluded. This measure ensures the model is accurate and reliable. Educational training and qualification along with legal and ethical principles encompass the methodology.

Copyright © Moniphia Hewling (eMRockOnline.com)

Screen Saver Screen

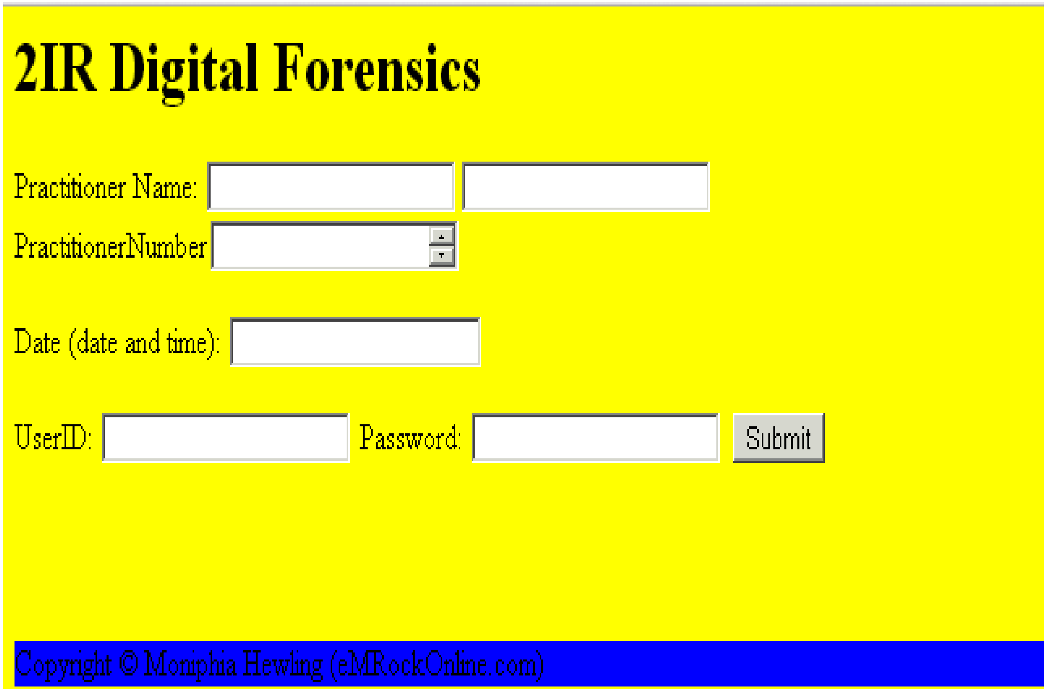


2IR

Digital Forensics Methdology

Moniphia Hewling 2013.

Log in Screen



2IR Digital Forensics

Practitioner Name:

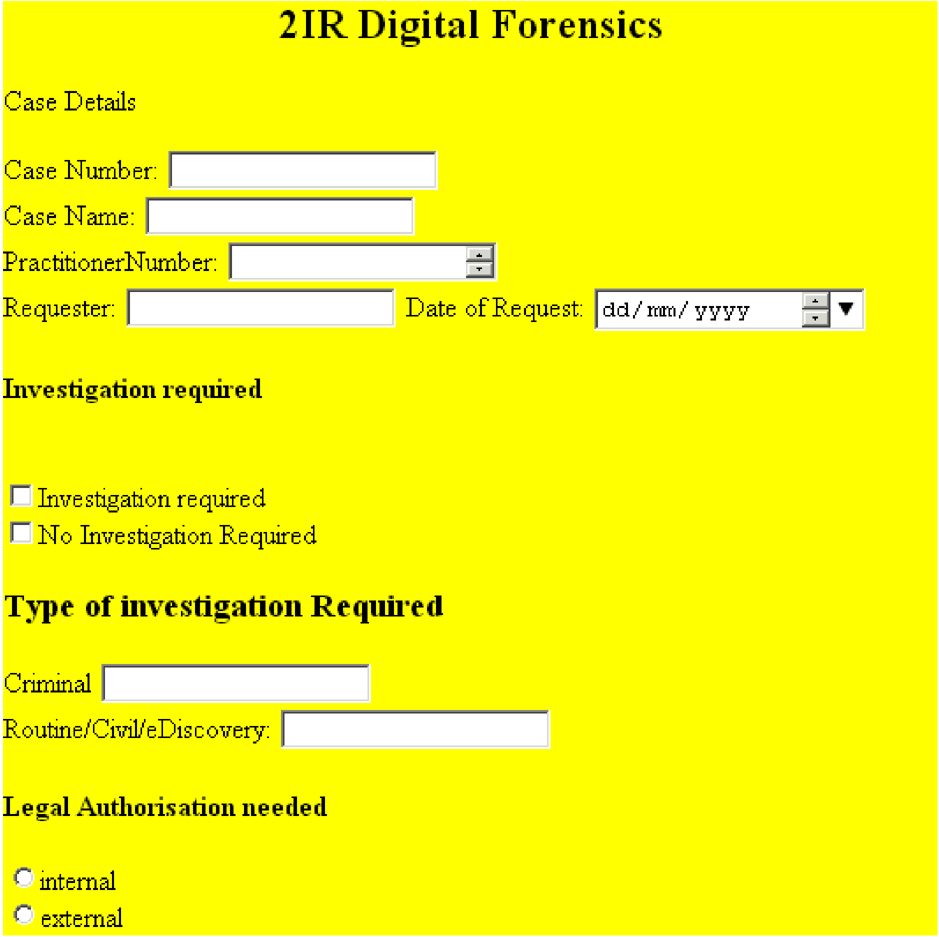
PractitionerNumber

Date (date and time):

UserID: Password:

Copyright © Moniphia Hewling (eMRockOnline.com)

Case Detail Screen



2IR Digital Forensics

Case Details

Case Number:

Case Name:

PractitionerNumber:

Requester: Date of Request: dd/mm/yyyy

Investigation required

□ Investigation required

□ No Investigation Required

Type of investigation Required

Criminal

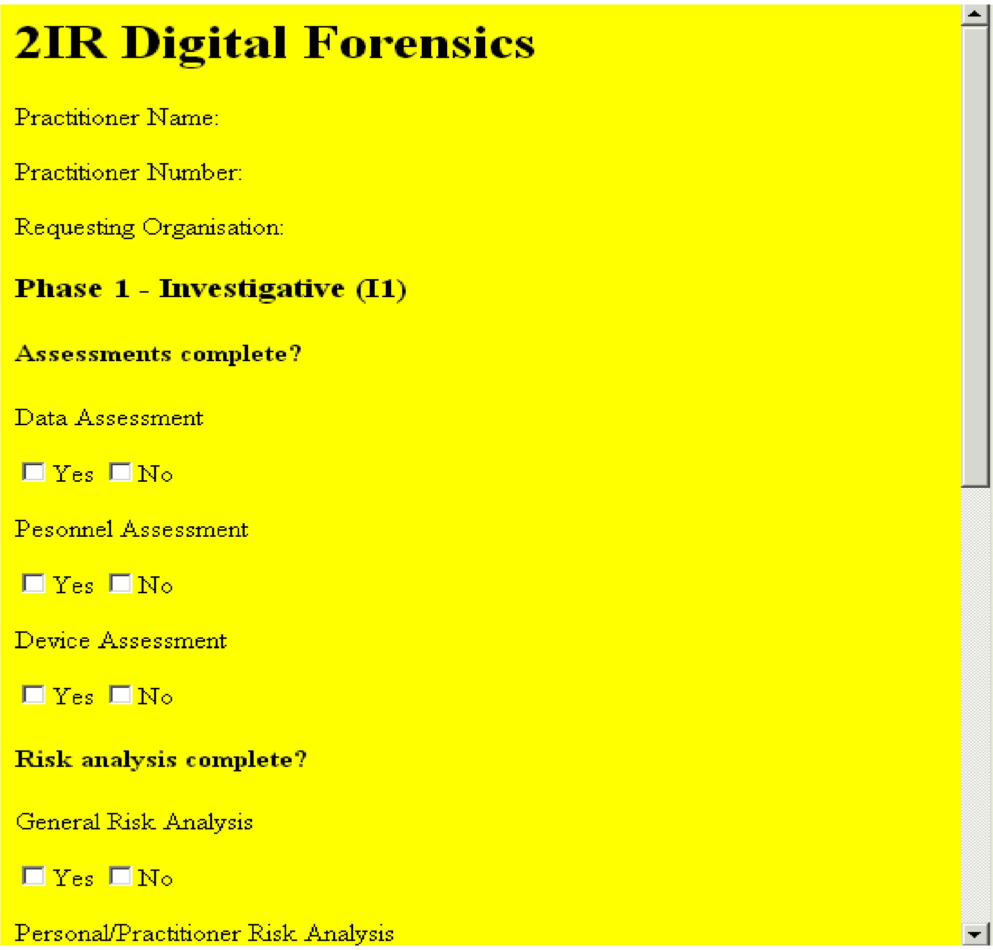
Routine/Civil/eDiscovery:

Legal Authorisation needed

○ internal

○ external

Phase one screen



2IR Digital Forensics

Practitioner Name:

Practitioner Number:

Requesting Organisation:

Phase 1 - Investigative (I1)

Assessments complete?

Data Assessment

□ Yes □ No

Pesonnel Assessment

□ Yes □ No

Device Assessment

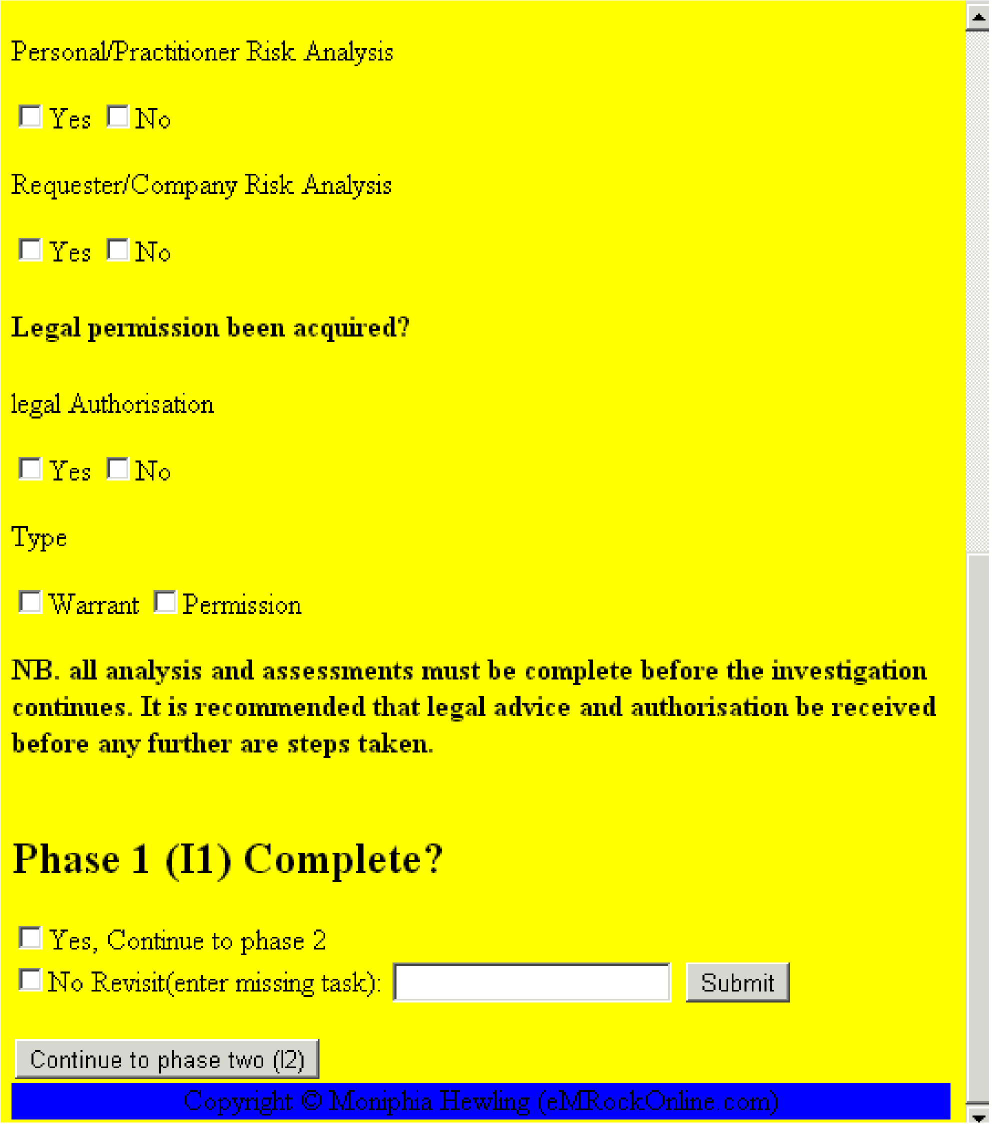
□ Yes □ No

Risk analysis complete?

General Risk Analysis

□ Yes □ No

Personal/Practitioner Risk Analysis



Personal/Practitioner Risk Analysis

□ Yes □ No

Requester/Company Risk Analysis

□ Yes □ No

Legal permission been acquired?

legal Authorisation

□ Yes □ No

Type

□ Warrant □ Permission

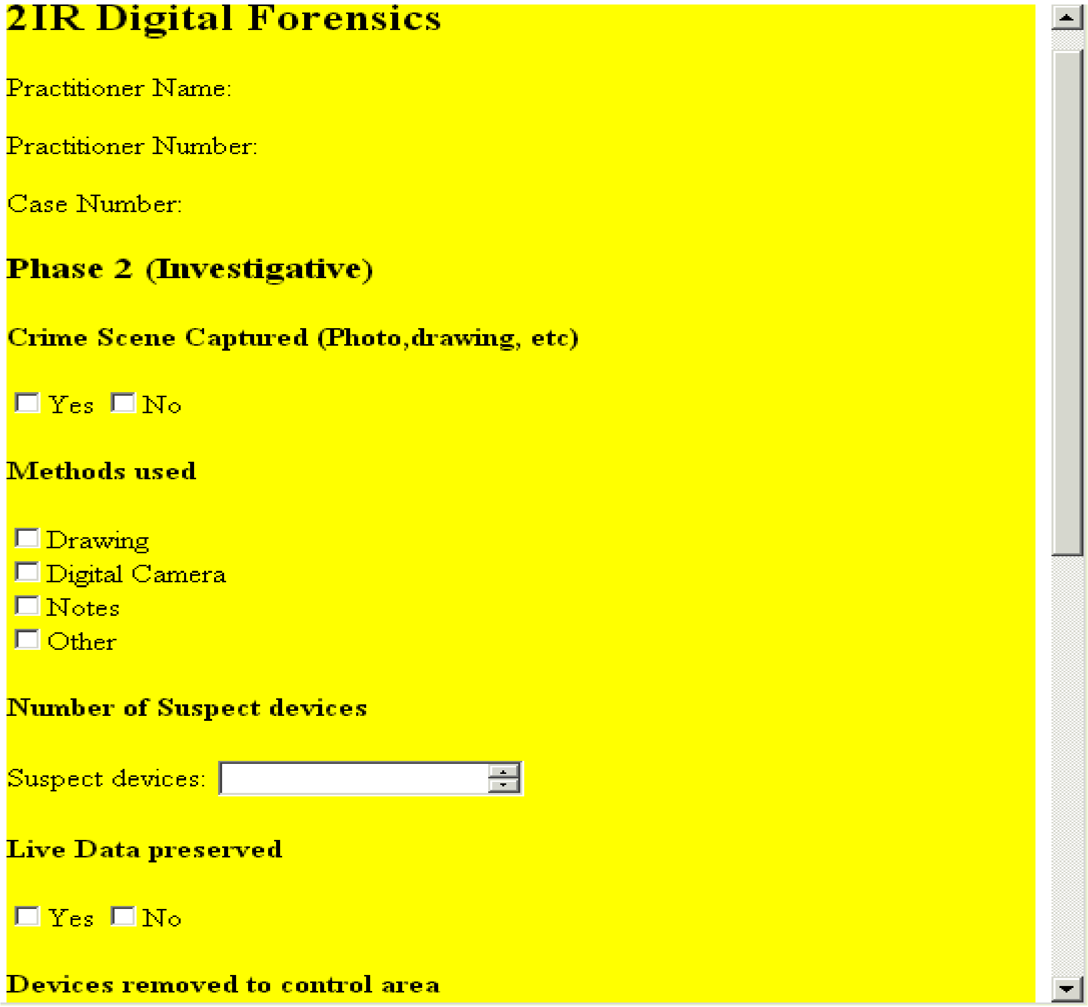
NB. all analysis and assessments must be complete before the investigation continues. It is recommended that legal advice and authorisation be received before any further are steps taken.

Phase 1 (I1) Complete?

□ Yes, Continue to phase 2
□ No Revisit(enter missing task): ▭ Submit

Copyright © Moniphia Hewling (eMRockOnline.com)

Phase two screen



2IR Digital Forensics

Practitioner Name:

Practitioner Number:

Case Number:

Phase 2 (Investigative)

Crime Scene Captured (Photo,drawing, etc)

□ Yes □ No

Methods used

□ Drawing
□ Digital Camera
□ Notes
□ Other

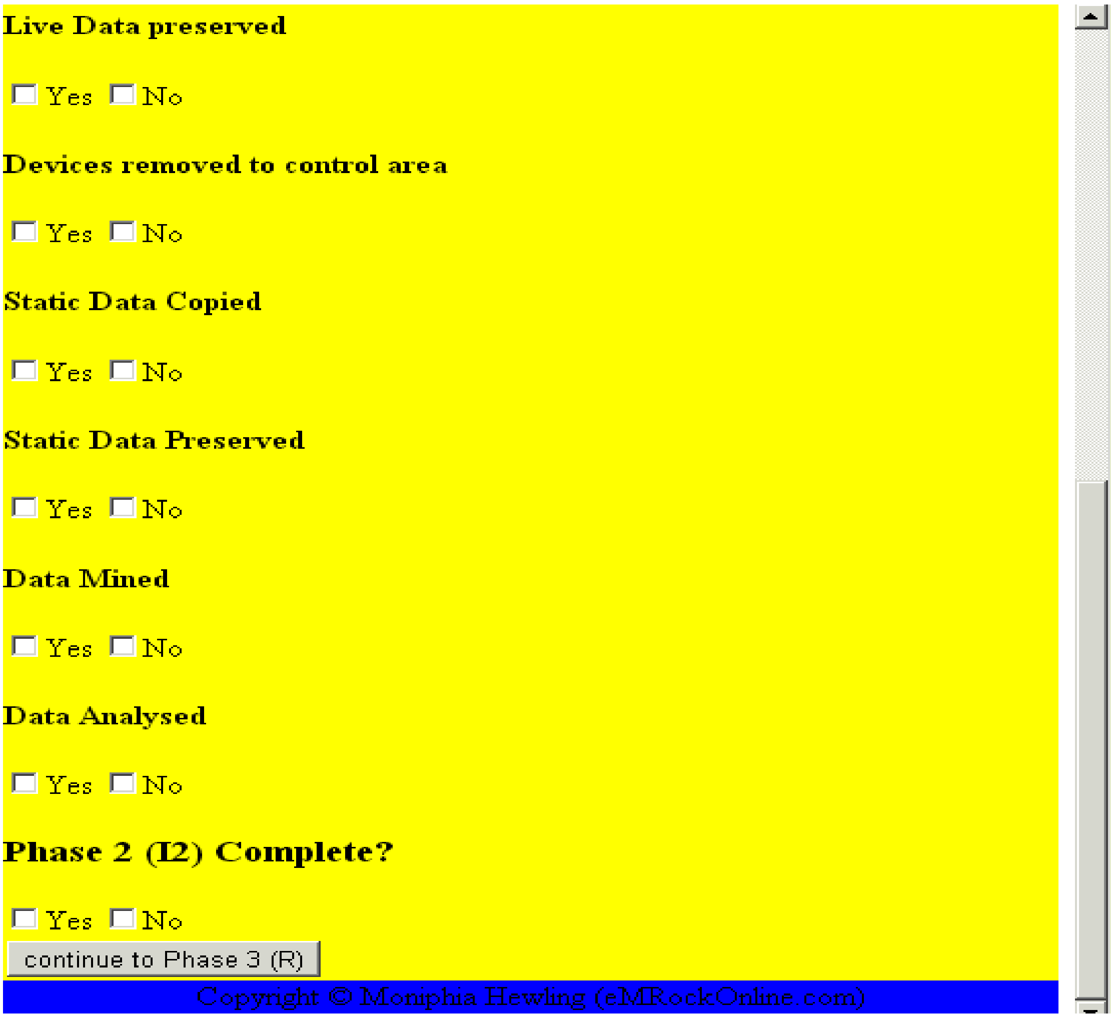
Number of Suspect devices

Suspect devices:

Live Data preserved

□ Yes □ No

Devices removed to control area



Live Data preserved

□ Yes □ No

Devices removed to control area

□ Yes □ No

Static Data Copied

□ Yes □ No

Static Data Preserved

□ Yes □ No

Data Mined

□ Yes □ No

Data Analysed

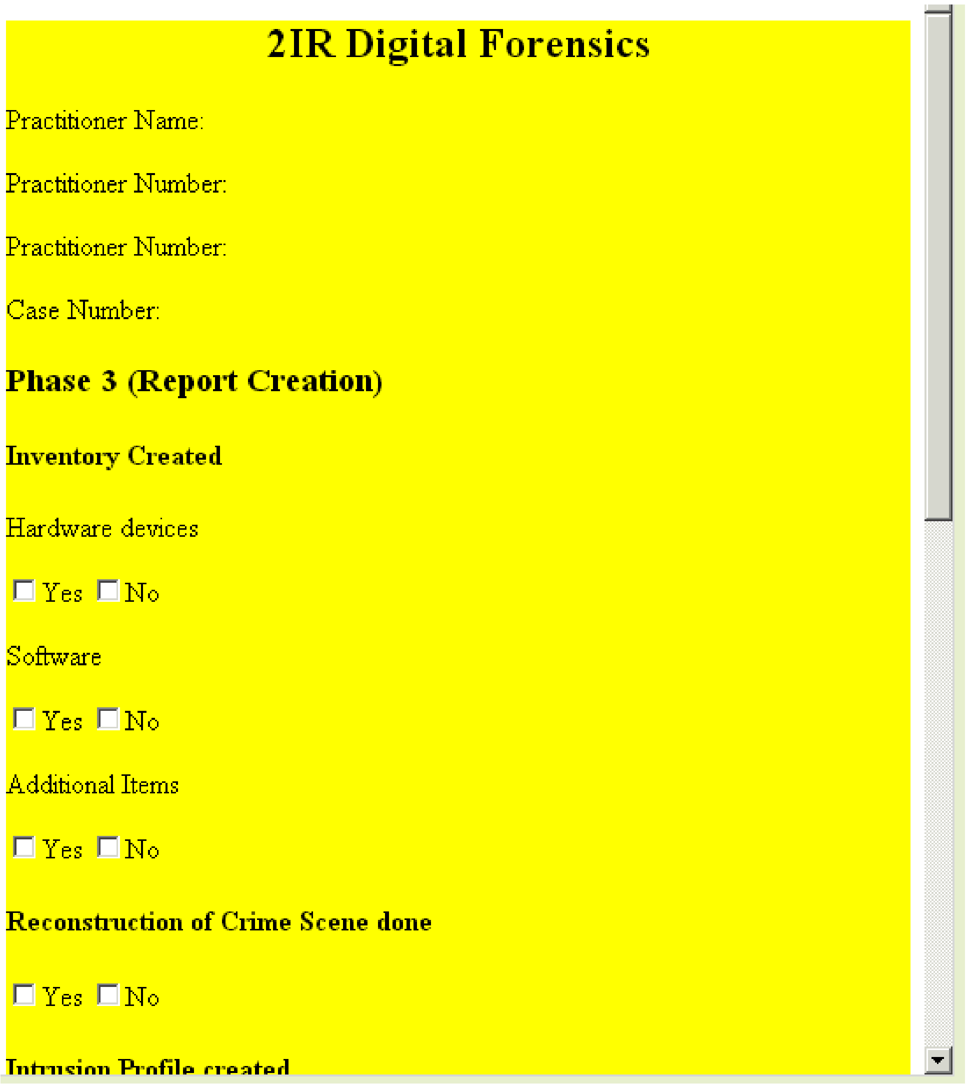
□ Yes □ No

Phase 2 (I2) Complete?

□ Yes □ No

Copyright © Moniphia Hewling (eMRockOnline.com)

Phase three Screen



2IR Digital Forensics

Practitioner Name:

Practitioner Number:

Practitioner Number:

Case Number:

Phase 3 (Report Creation)

Inventory Created

Hardware devices

□ Yes □ No

Software

□ Yes □ No

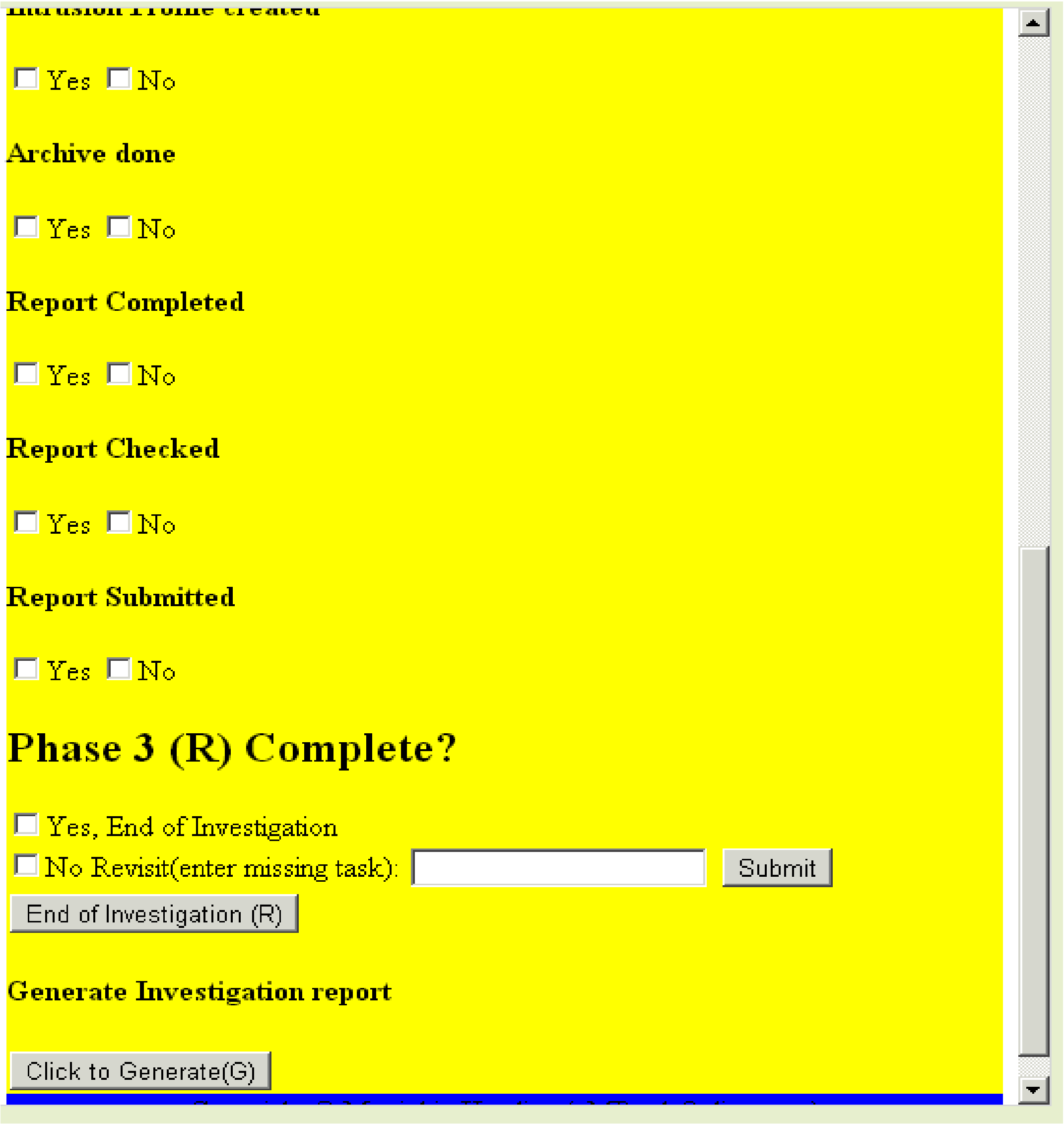
Additional Items

□ Yes □ No

Reconstruction of Crime Scene done

□ Yes □ No

Intrusion Profile created



Intrusion Profile created

□ Yes □ No

Archive done

□ Yes □ No

Report Completed

□ Yes □ No

Report Checked

□ Yes □ No

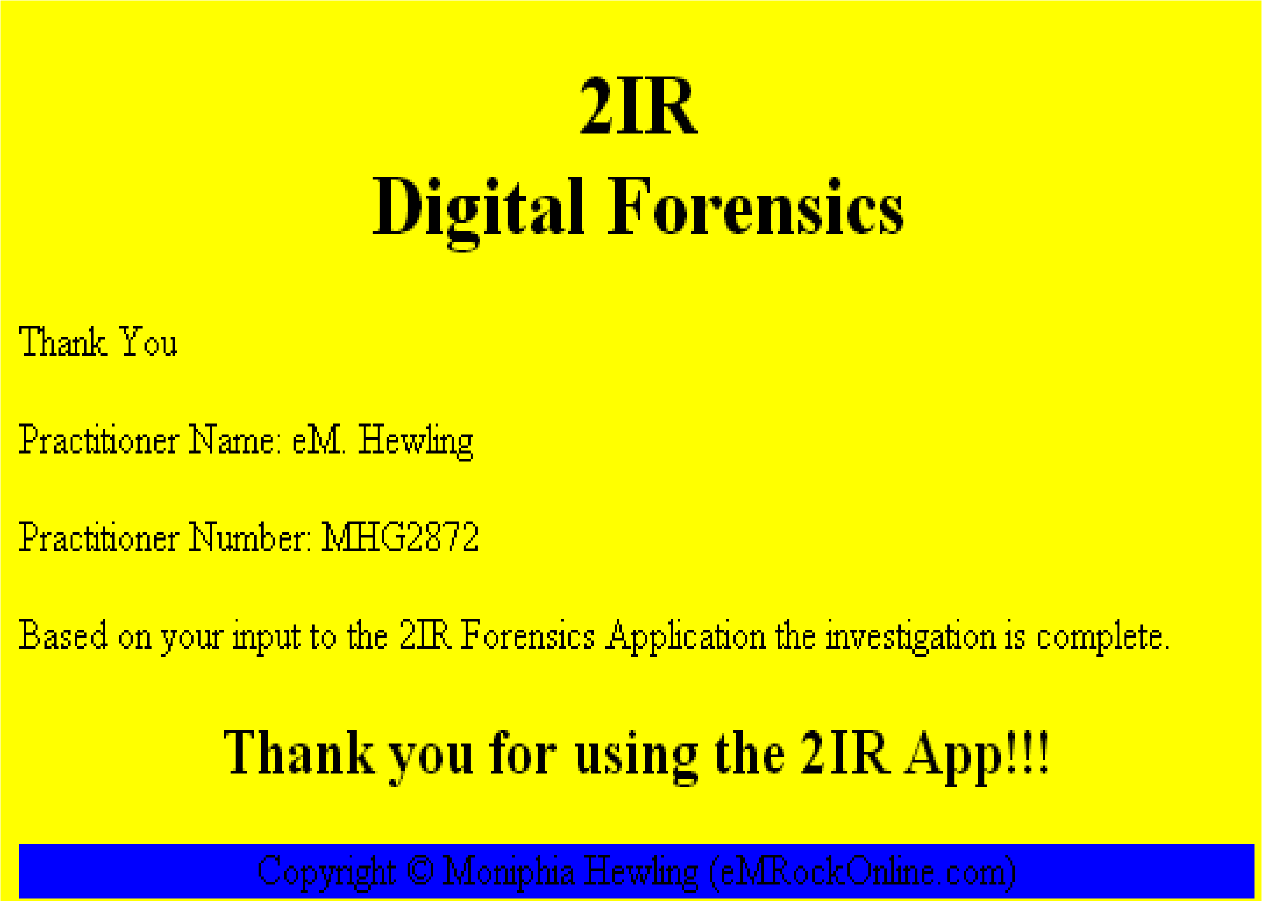
Report Submitted

□ Yes □ No

Phase 3 (R) Complete?

□ Yes, End of Investigation
□ No Revisit(enter missing task):

Generate Investigation report



2IR
Digital Forensics

Thank You

Practitioner Name: eM. Hewling

Practitioner Number: MHG2872

Based on your input to the 2IR Forensics Application the investigation is complete.

Thank you for using the 2IR App!!!

BIBLIOGRAPHY

ACPO., The Association of Chief Police Officers of England, Wales and Northern Ireland e-Crime strategy (2009) available on the 17th October 2009 athttp://www.acpo.police.uk/asp/policies/Data/Ecrime%20Strategy%20Website%20Version.pdf

Adelstein, F. Live forensics: diagnosing your system without killing it first. Commun. ACM 49 (February2006), 63–66.

Aeilts T., (2011) Defending against cybercrime and terrorism FBI law enforcement Bulletin. Available at http://www.au.af.mil/au/awc/awcgate/fbi/universities_fight_terrorism.pdf [Accessed on October 30, 2011]

Agarwal, M. A., Gupta, M. M., Gupta, M. S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. International Journal of Computer Science and Security (IJCSS), 5(1), 118.

Austin, R. D. (2007, September). Digital forensics on the cheap: teaching forensics using open source tools. In Proceedings of the 4th annual conference on Information security curriculum development (p. 6). ACM.

Bernstein, D. E. (2008). Expert witnesses, adversarial bias, and the (partial) failure of the Daubert revolution. George Mason University Law and Economics Research Paper No. 07-11. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?
abstract_id=963461

Bhaskar, R. (2006). State and local law enforcement is not ready for a cyber katrina. Communications of the ACM, 49(2), 81-83.

Biggs, S., & Vidalis, S. (2009, November). Cloud computing: The impact on digital forensic investigations. In Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for (pp. 1-6). IEEE.

Bogen, A. C., & Dampier, D. A. (2005). Unifying computer forensics modeling approaches: a software engineering perspective. In Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on (pp. 27-39). IEEE.

Burden K., Palmer C. (2004), Cyber crime - A new breed of criminal? Computer Law and Security Report, vol. ... 1(1), pp. 24-27

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. Psychological bulletin, 56(2), 81.

Carlton, G. H. (2006). A protocol for the forensic data acquisition of personal computer workstations. Unpublished doctoral dissertation, University of Hawaii, Honolulu.

Carlton, G. H. (2007). A grounded theory approach to identifying and measuring forensic data acquisition tasks. Journal of Digital Forensics, Security and Law, 2(1), 35-55.

Carrier B. D., Spafford E., (2004) 'An event based Digital forensics Investigation Framework' Center for Education and Research in Information Assurance and Security.

Carrier, B. (2002). Open source digital forensics tools: The legal argument. stake Research Report

Carrier, B. D. (2006). A hypothesis-based approach to digital forensic investigations. ProQuest.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. International Journal of digital evidence, 2(2), 1-20.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. International Journal of digital evidence, 2(2), 1-20.

Casey, E. (2004). Digital Evidence and Computer Crime, Forensic science, Computers and the Internet. Academic Press, London, UK

Casey, E. (2011). Digital Evidence and Computer Crime, Forensic science, Computers and the Internet. Academic Press, London, UK

CERT, U. (2008). US CERT Security Publications.

Chaikin D., (2007) Network Investigations of Cyber Attacks: The limits of digital evidence, Springer Science and Business Media

Charmaz, K. (2006). Constructing grounded theory: A practical guide through qualitative analysis. Thousand Oaks, CA: Sage.

Chisholm C. (2010) Integrating Forensics Investigation into e Discovery

Clarke R. J (2005) Research Models and methodologies Available at: http://www.uow.edu.au/content/groups/public [Accessed 04 September 12, 2013]

Cohen, F. (2008). Challenges to digital forensics evidence. Livermore, CA: ASP Press.

Cohen, L., Manion, L., & Morrison, K. (2011). Research methods in education. Routledge.
Craiger P., Ponte C., Whitcomb C., Pollitt M., Eaglin R., (2007) Master's Degree in Digital Forensics. In Proceedings of the 40th Hawaii International Conference on Systems Scientist.

Creswell, J. W. (2003) Research Design: Qualitative, Quantitative, and Mixed Method Approaches. Thousand Oaks, Calif.: London: Sage Publications.

CTOSE Cyber Tools On-Line Search for Evidence <http://www.ctose.org/info/index.html> at 12 October 2006.

Cuardhuain S. O., (2004) An Extended Model of Cyber Crime Investigation. Journal of Digital Evidence. Vol. 3. Issue 1

Daubert v Merrell Dow Pharmaceuticals, 1993, 509 US 579 Giannelli, Paul C., and Edward J. Imwinkelried. Scientific evidence. Michie Company, 1993.

DFRW, 2001 Digital Forensic Research Workshop. A road map for digital forensic research. Report from the First Digital Forensic Research Workshop, August 2001, Utica, New York; 2001.

Dick, B. (2005). Grounded theory: A thumbnail sketch., from Action Research and action learning for community and Organisational change. [Available at: http://www.scu.edu.au/schools/gcm/ar/arp/grounded.html. Accessed on September 3, 2012

Digital Forensic Research Workshop. A road map for digital forensic research. Report from the First Digital Forensic Research Workshop, August 2001, Utica, New York; 2001. (DFRW)

Elliott, N., & Lazenbatt, A. (2005). How to recognise a "quality" grounded theory research study. Australian Journal of Advanced Nursing, 22(3), 48-52.
Filstead, W. J. (1979). Qualitative methods: A needed perspective in evaluation research. Qualitative and quantitative methods in evaluation research, 33-48.

Forensics Science and Crime Science. Available at: http://www.staffs.ac.uk/academic_depts/sciences/subject/forensics/. Accessed September 3, 2010

Forensics Science Regulator – GOV.UK 2010 Available at: https://www.gov.uk/government/organisation/forensic-science-regulator [Accessed September 9, 2010]

Frechtling J and Sharpe L (1997) User Friendly Handbook for Mixed Method Evaluations. Available at http://www.nsf.gov.pubs/1997/nsf97153. Accessed March 4, 2013
Frye v. United States, 54 App. D.C. 46, 293 F.1013 (1923).

Fulbright and Jowoski L., (2006) Third Annual Litigation Trends Survey Findings. Available from: http://www.fullbtight.com/mediaroom/file/2006. Accessed on May 12 2010

Gerring, J. (2001) Social Science Methodology: A Criterial Framework.
Cambridge: Cambridge University Press.

Giordano, J., & Maciag, C. (2002). Cyber forensics: A military operations perspective. International Journal of Digital Evidence, 1(2), 1-13.

Hall, B. And Howard, K. (2008) A Synergistic Approach: Conducting Mixed Methods
Research With Typological and Systemic Design Considerations. Journal of
Mixed Methods Research, 2(3) 248-269.

Hewling (2010), Digital Forensics: The UK Legal Framework, Published Masters dissertation, University of Liverpool, Liverpool UK

Hewling, M. O., Sant, P. (2011), Digital Forensics: The need for integration. Proceedings of Digital Forensics & Incident Analysis (WDFIA 2011)

http://www.iacis.org/ International Association for Computers and Information Systems (IACIS)

Huber, R., Snider, A. And Lawrence, E. (2005) Influencing Through Argument.
NY: Central European University Press

Huebner, E., Bem, D., & Bem, O. (2007). Computer Forensics–Past, Present And Future. Information Security Technical Report, 8(2), 32-46.

Ieong, R. S. (2006). FORZA–Digital forensics investigation framework that incorporate legal issues. digital investigation, 3, 29-36.

International Organization on Computer Evidence. Digital evidence, standards and principles; 2003. Available from: http://www.fbi.gov. (IOCE) Accessed on August 20, 2010

Johnson, B., & Turner, L. A. (2003). Data collection strategies in mixed methods research. Handbook of mixed methods in social and behavioral research, 297-319.

Johnson, R., Onwuegbuzie, A. And Turner, L. (2007) Toward a Definition of Mixed

Methods Research. Journal of Mixed Methods Research, 1(2) 112-133.

Joppe M (2000) The Research Process. Available at: http://www.ryerson.ca/~mjoppe/rp.htm Accessed on December 20, 2012

Kenneally, Erin E., and Christopher LT Brown. "Risk sensitive digital evidence collection." Digital Investigation 2.2 (2005): 101-119.

Kerr, O. S. (2009). Computer crime law (2nd ed.). St. Paul. MN: Thomson/West.

Kerr, Orin. "Searches and seizures in a digital world." Harvard Law Review 119 (2005): 531.

Kessler, G. C. (2010). Judges' awareness, understanding, and application of digital evidence (Doctoral dissertation, Nova Southeastern University).

Kessler, G. C., & Haggerty, D. (2008). Pedagogy and Overview of a Graduate Program in Digital Investigation Management. In Hawaii International Conference on System Sciences, Proceedings of the 41st Annual (pp. 481-481). IEEE.

King G. (2006) Forensics Plan Guide, SANs Reading Room. Available online at http://www.sans.org/reading-room/whitepapers/forensics [accessed on May 4, 2012]

Kohl, U. (1999) 'Legal reasoning and Legal change in the age of the Internet—Why the ground rules are still valid, International Journal of Law and IT. Vol. 7 (June, 1999) Available at http://www.liv.ac.uk/library/ohecampus/ Accessed on July 30 2010

Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated Digital Forensic Process Model. Computers & Security.

Köhn, M., Eloff, J. H., & Olivier, M. S. (2008, July). UML Modelling of Digital Forensic Process Models (DFPMs). In ISSA (pp. 1-13).

Kruse W. Heiser J. G. (2001). Computer Forensics: Incident Response Essentials (1st ed.), Addison Wesley Professional. USA

Kuchta K. J., (2000) 'Computer Forensics Today' Law, Investigations and Ethics Available from: http://www.liv.ac.uk/library/ohecampus/ Accessed on July 30, 2010

Kuhn, T. S. (1970). Logic of discovery or psychology of research. Criticism and the Growth of Knowledge, 1-23.

Lancaster, G. (2005) Research methods in management: a concise introduction to research in management and business consultancy. Oxford: Elsevier Butterworth-Heinemann.

Lee H, C., Palmbeach T. M., Miller M. T. (2001) Henry Lee's crime scene handbook. Elsevier Academic Press Available from: http://academic.evergreen.edu/curricular/social_dilemmas/fall/Readings/Week_06/Crime%20Scene%20Handbook.pdf Accessed on September 28, 2012

Lloyd I, (2004) Information Technology Law, oxford University Press Inc, New York

Manes, G. W., & Downing, E. (2009). Overview of licensing and legal issues for digital forensic investigators. Security & Privacy, IEEE, 7(2), 45-48.

Manes, G. W., Downing, E., Watson, L., & Thrutchley, C. (2007). New federal rules and digital evidence. In G. Dardick (Ed.), Proceedings of the Conference on Digital Forensics, Security and Law (pp. 31-40). Farmville, VA: Longwood University.

Marshall A. (2011) Standards, regulations and quality in digital investigations: the state we are in. Available at http://sciencedirect.com/science/article/piis1742287611000880. Accessed on September 4, 2012

Mason S, (2013), BCS Workshop on Cyber crime, Canterbury Christ Church University, Canterbury, UK

Mason, D., Carlin, A., Ramos, S., Gyger, A., Kaufman, M., Treichelt, J., (2007). Is the open way a better way? Digital forensics using open source tools. The Computer Society. 1-10.

Maxwell, J. and Loomis, D. (2003) Mixed methods design: An alternative approach. In: A. Tashakkori and C. Teddlie [Eds.]: Handbook of mixed methods in social and behavioral research. Thousand Oaks CA: Sage Publications.

Mercer L. D., (2004) Computer Forensics, Characteristics and preservation of Digital Evidence. FBI Law Enforcement Bulletin. Available from: http://www.liv.ac.uk/library/ohecampus/ Accessed on June 11, 2011

Meyers, L., Gamst, G. and Guarino, A. (2005) Applied Multivariate Research: Design and Interpretation. London: Sage Publications.

Meyers, M., & Rogers, M. (2004). Computer forensics: the need for standardization and certification. International Journal of Digital Evidence, 3(2), 1-11.

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook (2nd ed.). Thousand Oaks, CA: Sage.

Morgan, D. (1998) Practical Strategies for Combining Qualitative and Quantitative Methods: Application to Health Research. Qualitative Health Research, 8(3) 362-376.

Morgan, S. J., & Symon, G. (2004). Electronic interviews in organizational research. Essential guide to qualitative methods in organizational research, 23-33.
N. Beebe, J. Clark 2005 A hierarchical, objectives-based framework for the digital investigations process Elsevier Digital Investigation (2005) 2, pp. 147–167

Nance, K., Hay., B., & Bishop, M. (2009). Digital forensics: Defining a research agenda. In R. Sprauge (Ed.), Proceedings of the Forty-Second Annual Hawai'i International Conference on System Sciences. Los Alamitos, CA: IEEE Press.

Nance, K., Hay., B., & Bishop, M. (2009). Digital forensics: Defining a research agenda. In R. Sprauge (Ed.), Proceedings of the Forty-Second Annual Hawai'i International Conference on System Sciences. Los Alamitos, CA: IEEE Press.

National Criminal Justice System (nd) National Criminal Justice Reference Service Available at https://www.ncjrs.gov/ Accessed September 3, 2013.

National Institute of Justice.(July 2001) Electronic Crime Scene Investigation A Guide for First Responders. Available from http://www.ncjrs.org/pdffiles1/nij/187736.pdf. Accessed on July 22, 2011

Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and examining computer forensic evidence. Forensic Science Communications,2(4), 1-13.

Osborne, G.; Turnbull, B.; Slay, J., "The "Explore, Investigate and Correlate' (EIC) Conceptual Framework for Digital Forensics Information Visualisation," Availability, Reliability, and Security, 2010. ARES '10 International Conference on , vol., no., pp.629,634, 15-18 Feb. 2010
doi: 10.1109/ARES.2010.74 Available from
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5438026&isnumber=5437988
Accessed on January 12, 2011

Palmer, G. (2001) A Road Map for Digital Forensics Research. Digital Forensic Research Workshop (DFRWS) Technical Report (DTR) T001-01 Final. Retrieved from http://www.dfrws.org/2001/dfrws-rm-final.pdf

Pandit, N. R. (1996). The creation of theory: A recent application of the grounded theory method. The qualitative report, 2(4), 1-14.

Patton, M. Q. (1990). Qualitative evaluation and research methods . SAGE Publications, inc.
Peisert, S., Bishop, M., & Marzullo, K. (2008,). Computer forensics in forensis. In Systematic Approaches to Digital Forensic Engineering, 2008. SADFE'08. Third International Workshop on (pp. 102-122). IEEE.

Perumal S., (2009) Digital Forensics Model Based on Malaysian Investigation Process, IJCSNS Vol. 9 No. 8 Available from www.sciencedirect.com

Pollitt M., (1995) Principles, Practices, and Procedures: An approach to standards in computer forensics. Available from; www.digitalevidencepro.com/resources/principles.pdf

Prichard, J. J., & MacDonald, L. E. (2004). Cyber terrorism: A study of the extent of coverage in computer security textbooks. Journal of Information Technology Education, 3, 279-289.

R. Leong FORZA – Digital forensic investigation framework that incorporate legal issues Digital Investigation 3S (2006), pp. S29–S36

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. International Journal of Digital Evidence, 1(3), 1-12.

Ricci I. S. C. (2006) Digital Forensics Framework that incorporate legal issues. Available from www.sciencedirect.com Accessed on October 20, 2010

Rogers, M. (2003). The Psychology of Cyber-Terrorism. Terrorists, Victims and Society: Psychological Perspectives on Terrorism and its Consequences, 77-92.

Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. Computers & Security, 23(1), 12-16.

Saferstein, R. (2009). Forensics science: From the crime scene to the crime lab. Upper Saddle River, NJ: Pearson Education.

Sale, J., Lohfeld, L., and Brazil, K. (2002) Revisiting the Quantitative-Qualitative
Debate: Implications for Mixed-Methods Research. Quality and Quantity,
36(1) 43-53.

Salemat S. R. Yusof R. Sahib S. (2008) Mapping Process of Digital Forensic Investigation Framework. International Journal of Computer Science and Network Security Vol. 8 NO 10

Available from www.sciencedirect.com Accessed on October 30, 2010

Sartin B. (2006) Computer Forensics Digital Detectives Available at: http://www.scmagazineuk.com/computer-forensics-digital-detectives/article/106988/ Accessed on June 10, 2010

Schatz, B. (2007). BodySnatcher: Towards reliable volatile memory acquisition by software. digital investigation, 4, 126-134.

Schatz, B. L. (2007). Digital evidence: representation and assurance.

Scientific Working Group on Digital Evidence (SWGDE) of the National Center for Forensic Science (NCFS). Available at: http://ncfs.org/swgde/documents/swgde2006/Best_Practices_for_Computer_Forensics%20V2.0.pdf Retrieved on July 20, 2010

Scientific Working Group on Digital Evidence. SWGDE draft best practices; 2002. Available from: http://ncfs.ucf.edu/digital_evd.html. Accessed on July 20, 2010

Sekaran, U. (2003) Research Methods for Business: A Skill Building Approach.
USA: John Wiley and Sons.

Sieber, S. D. 1973 "The integration of fieldwork and survey methods." Ameri- can Journal of Sociology, 78: 1335-1359.

Stahl, B. (2008) Information Systems: Critical Perspectives. London: Rotledge.

Trochim, W. M., Donnelly, J. P. , (2008). Research methods knowledge base. Mason, OH: Atomic Dog/Cengage Learning.

Tu, P.H., Kelliher T.P., Miller K. W., Taister M.A., (2003) Towards a statistical basis for facial deformation modes in reconstruction Forensic Sci. Int., 136 (Suppl. 1) (2003), pp. 168–169

Tu, M., Cronin, K., Xu, D., (2013) On the development of a Digital Forensics Cyrriculum. Available at http://www.dsu.edu/research/ia/documents/%5B6%5D-On-the-development-of-Digital-Forensics-Curriculum.pdf Accessed on March 12, 2012

Turvey, B. E. (Ed.). (2011). Criminal profiling: An introduction to behavioral evidence analysis. Access Online via Elsevier.

U.S. Courts. (2008a). Federal rules of civil procedure. Administrative Office of the U.S.

Courts. Washington, DC: U.S. Government Printing Office. Retrieved May 5, 2010, from http://www.uscourts.gov/rules/CV2008.pdf

UK Information Security Breaches Survey Results 2012. 2013 [ONLINE] Available at:http://www.pwc.co.uk/audit-assurance/publications/uk-information-security-breaches-survey-results-2012.jhtml. [Accessed 11 July 2013].

US CERT 2008 Available from: http://www.us-cert.gov/security-publications [Accessed on March 8, 2012]

UK Copyright Law, A summary. Available from http://www.copyrightservice.co.uk/copyright/uk_law_summary (Accessed on, January 21, 2012)

Walker, C. (2007). Computer forensics: bringing the evidence to court. Online: http://www. infosecwriters. com/text_resources/pdf/Com puter_Forensics_to_Court. pdf as on, 12.

Weber, R. (2004) The Rhetoric of Positivism Versus Interpretivism: A Personal View. [Editor's Comments]. MIS Quarterly, 28 (1) iii – xii.

White, P. C. (2010). Crime scene to court: the essentials of forensic science. Royal Society of Chemistry.

Yanisec A, Erbacher R. F., Marks D. G. Pollitt M., Sommer P. (2003) Computer Forensics Education, IEEE Security and Privacy

Yong-Dal S., (2008) New Digital Forensics Investigation Procedure Model. Proceedings of Fourth International Conference on Networked Computing and Advanced Information Management. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4624063 Accessed on March 12, 2011

Cases

Debtor American Express Travel Related Services Company, Inc v Vee Vinhee (2005) http://quest.law.com/ /jsp/ca/LawDecision

Zubulake v UBS Warburg (2003) [http://lawschool.courtroomview.com]

Coleman Holdings Inc v Morgan Stanley.(2005) http://www.ediscoverylaw.com

United States v Carey (1998) [http://laws.findlaw/10th/983077.htm]

United States v Benedict [http://www.cybercrime.gov/]

Aston Investments v OJSC Russian Aluminum (2006) [http://www.deaeslr.org/2008.html]

Four seasons v Consorcio Bar (2003) [http://www.laws.lp.findlaws.com]

R v Cochrane (1993) [http://www.hse.gov.uk/enforce/Enforcementguide]

United States v Councilman (2004) [digital.law.washington.edu/dspace-law]

State of Florida vs. Case Anthony (2011) http://lawrecord.com/2011/08/11/the-case-of-casey-anthony-defending-the-american-jury-system/