Integrating Behavioural Analysis within the Digital Forensics Investigation Process

by

Noora Ahmad Al Mutawa

A thesis submitted in partial fulfilment for the requirements for the degree of Doctor of Philosophy at the University of Central Lancashire

October 2018

DECLARATION AND PUBLICATIONS

STUDENT DECLARATION FORM

Concurrent registration for two or more academic awards

I declare that while registered as a candidate for the research degree, I have not been a registered candidate or enrolled student for another award of the University or other academic or professional institution

Material submitted for another award

I declare that no material contained in the thesis has been used in any other submission for an academic award and is solely my own work

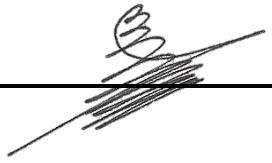
Published material

Some of the material contained in this thesis has been published as professional conference and journal papers as follows:

1. Al Mutawa, N., Bryce, J., Franqueira, V. N. L., & Marrington, A. (2015, August). Behavioural evidence analysis applied to digital forensics: An empirical analysis of child pornography cases using P2P networks. In *Availability, Reliability and Security (ARES), 2015 10th International Conference on* (pp. 293-302). IEEE.

2. Al Mutawa, N., Bryce, J., Franqueira, V. N. L., & Marrington, A. (2016). Forensic investigation of cyberstalking cases using Behavioural Evidence Analysis. *Digital Investigation*, *16*, S96-S103.

3. Franqueira, V. N. L., Bryce, J., Al Mutawa, N., & Marrington, A. (2017). Investigation of Indecent Images of Children cases: Challenges and suggestions collected from the trenches. *Digital Investigation*.

Signature of Candidate 

Type of Award **Doctor of Philosophy**

School **School of Physical Sciences and Computing**

DEDICATION

Every challenging work needs self-efforts as well as support from those who are very close to our heart.

My humble effort I dedicate to my beloved

Father & Mother

Whose affection, love, encouragement and prayers made me able to achieve such success and honour.

ABSTRACT

This programme of research focused on incorporating Behavioural Analysis (BA) within the digital forensics investigation process. A review of previously developed digital forensics investigation models indicated a lack of sufficient consideration of the behavioural and motivational dimensions of offending, and the way in which digital evidence can be used to address these issues during the investigation process. This programme of research aimed to build on previous work by scientific researchers and investigators by developing a digital forensics investigation model which incorporates greater consideration of the behavioural and motivational implications of case-related digital evidence based on current theoretical understandings of these aspects of offending from forensic psychology. This can aid with understanding of the crime events and reconstruction, and lead to the development of more detailed models and guidelines for examining computer-facilitated interpersonal crimes.

The first study employed an abductive approach to forensically analyse individual cases (real cases obtained from the Dubai Police archives) applying BA to the online Sexually Exploitative Imagery of Children (SEIC) and cyberstalking. Its aim was to investigate what BA could contribute to the digital forensics investigation of cases within these crime categories. It identified five benefits: (1) providing focus, speed and investigative directions, (2) inferring victim/offender behaviours, (3) inferring offender motivation(s), (4) identifying potential victims, and (5) eliminating suspects. This was followed by a survey study empirically examining the perceptions of national and international digital forensics practitioners regarding the use and utility of BA during the process of investigating SEIC and cyberstalking cases. The results indicated that while the majority believed that BA has potential to contribute to many aspects of digital forensics investigations, their daily investigative activities involved a limited use of this technique. The implications of the study were outlined, and emphasised the need to design a digital forensics investigation model that provides guiding steps and illustrations on how to utilise BA in digital forensics investigations.

Based on the findings from the conducted studies, a digital forensics investigation model that incorporates aspects of BA was designed. It aimed to provide a pragmatic, structured, multidisciplinary approach to performing a post mortem examination, analysis, and interpretation of the content of the digital devices associated with computer-facilitated interpersonal crimes. Two comprehensive case studies were also used to illustrate the investigative importance of the model in investigating computer-facilitated interpersonal crimes.

ACKNOWLEDGEMENTS

I would like to thank all the people without whom this project would never have been possible.

First, I would like to express my sincere gratitude to my supervisor: Dr Joanne Bryce, Dr Janet Read, Dr Virginia Franqueira, and Dr Andrew Marrington. Dr Joanne Bryce provided immeasurable guidance and support throughout the entire process. She has been insightful, encouraging and always available. She constantly helped me to remain focused on achieving my goal, and was always there to clarify my doubts despite her busy schedules. Her deep insights helped me at various stages of my research. I also remain indebted to her for her kind and encouraging words during times when I felt overwhelmed and under pressure. I feel privileged to have worked on my doctoral programme under her guidance and to have learnt from her research expertise.

Dr Janet is one of the most warm-hearted, positive, and encouraging people I know. She became my supervisor when I was halfway through my thesis. She provided guidance on the overall framework of my research, always boosted my confidence in my work, and really helped put me at ease on the day of the examination. I really appreciate her face-to-face meetings to discuss my thesis, and I remain amazed at her instant invaluable insights and suggestions. She is an inspiration!

Dr Virginia Franqueira provided countless hours of reflection, reading, encouragement, throughout the process. I appreciate not only her insightful comments, but also her constructive criticism and questions which helped improve and polish my research from various perspectives. Dr Andrew Marrington was my local supervisor, in Dubai. His guidance, feedback and suggestions were always invaluable. His door was always open whenever I needed, and he supported my research in any way he could. I truly appreciate him arranging a session at Zayed University on statistical analysis, correlation and multiple regression to help me analyse the collected data.

I also thank my supervisors for the countless meetings to discuss and enrich my research, and for encouraging me to write and publish my work. I am blessed to have had this extraordinary supervisory team for my PhD study and I immensely value their contributions and guidance.

I am also hugely appreciative to academics, especially Dr Rafael Brown, and digital forensic professionals who assisted me with this project. Their enthusiasm and willingness to provide interesting feedback made the completion of this research an enjoyable experience.

My sincere thanks to Dubai Police for providing scholarships to pursue doctoral studies, particularly to the late Commander-in-Chief of Dubai Police, Lieutenant General Khamis Al Mazeina (peace be upon his soul) for his continuous encouragement to gain knowledge. I would also like to express my gratitude to the Director of Digital Forensics Lab, Lt. Col. Rashed Lootah who gave me access to the digital forensics laboratory and research resources and facilities. Without his precious support it would not have been possible to conduct this research.

Finally, I would not have been able to complete this work without some amazing people for whose help I am immeasurably grateful: my parents, Ahmad and Mona, whose love and guidance are with me in whatever I pursue. They started me on the path of education a long time ago, and have encouraged and supported my studies ever since. A special feeling of gratitude to my sisters, brothers, and close friends for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. Most importantly, I wish to thank my loving and supportive husband, Hussain, and my three wonderful children, Maitha, Maryam and Ahmad, for their tolerance and patience, and for putting up with me being a part-time mother for such a very long time.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BA	**Behavioural Analysis**
BEA	Behavioural Evidence analysis
DF	Digital Forensics
DFIM	Digital Forensics Investigation Model
GPS	Global Positioning System
IP	Internet Protocol
MO	Modus Operandi
SEIC	Sexually Exploitative Imagery of Children
VoIP	Voice Over IP

1 INTRODUCTION

The proliferation of technology in modern society has caused revolutionary changes in every sector and institution, social communication, and lifestyle. A report from the Office for National Statistics (2017) stated that 90% of the UK's households had Internet access, showing an increase from 57% in 2006. It also stated that 73% of adults access the Internet while away from their homes through smartphones, an increase of 37% from 2011. Further, it was reported that 77% of adults had made purchases of goods or services online, compared to 53% in 2008. The Ontario Centre for International Governance Innovation reported that one in three Internet users are children (Livingstone et al., 2016). A report by The Office of Communications in the UK showed that 23% of children aged 8-11 and 72% of children aged 12-15 have a social media profile (Ofcom, 2016). The report also revealed an increase in children's use of group messaging services such as WhatsApp, Instagram, and Facebook Messenger. Finally, surveys conducted in the US by Pew Research Center between 2000-2016 showed that at the current time 9 in 10 US citizens use the Internet, 77% own a smartphone, and 69% own social media profiles (Smith, 2017). This advancement in the use and adaptation of technology has also influenced misconduct and encouraged criminal behaviour.

Despite the benefits of the Internet, its rapid evolution has created unparalleled opportunities for crime and misuse. The online environment possesses a number of properties that facilitate and encourage criminal behaviour. It efficiently connects individuals regardless of their geographical locations, allowing them to form relationships, pursue interests, and enjoy a virtual life (Casale and Fioravanti, 2015, Dutta et al., 2015, Rogers et al., 2006). Also, it provides anonymity which reduces the risk of being exposed, thus encouraging criminal behaviour (Malamuth et al., 2013). Disinhibition is another characteristic of the online environment which influences behaviour by giving individuals the opportunity to separate their online personality and acts from their actual real life and identity, making them feel less vulnerable about self-

disclosing and acting out (Agustina, 2015, Suler, 2004). Individuals with deviant intentions (e.g., fraudsters, cyberstalkers) can use social networks or online games as a place to groom potential victims, or to monitor the activities of their targets. They can hide their criminal intentions behind beautiful avatars and lure naive users into their traps (Rashid et al., 2013). Similarly, offenders motivated by monetary gain can infiltrate online profiles of targeted individuals, then tailor different scamming methods to induce them into making financial payments for promised goods, services, or investments (Abbasi et al., 2010, Buchanan and Whitty, 2014, Vahdati and Yasini, 2015).

The nature of the online environment also encourages individuals to participate in behaviour that can place them at risk. In online communities, millions of users share their personal information such as their age, gender, interests, locations, schedules, and whereabouts (Chen et al., 2016). As mentioned in the preceding paragraph, offenders and users with malicious intentions can use this information to their advantage in selecting their targets and committing offences. Interacting with online strangers, confiding in them, discussing private matters and problems, and sharing other personal information can also put users at the risk of being targets of online predators (Sampasa-Kanyinga and Hamilton, 2015, Suler, 2004). Other online behaviours that increase risk of victimisation that have been identified in the literature are increased use of social networking sites (Chen et al., 2017), online information disclosure (Van Wilsem, 2011), online shopping (Aghekyan-Simonian et al., 2012), downloading files from unreliable sources (Holt and Bossler, 2008), and opening emails from unknown sources (Chen et al., 2017).

Cybercrime, also known as digital or computer-facilitated crimes, refers to a wide range of criminal behaviour facilitated through digital devices and the Internet (Holt, 2016). A well-recognised classification of cybercrimes was proposed by Wall (2001), who categorised them into four groups based on the criminal behaviour associated with each type: (1) cyber-trespass, (2) cyber-deception and theft, (3) cyber-porn and obscenity, and (4) cyber-violence. Cyber-trespass is associated with offences related to the use of techniques and utilities to gain unauthorised access to computer systems, networks, and email accounts (e.g., hacking) (Holt, 2016). Cyber-deception and theft refers to the utilisation of techniques that facilitate the illegal acquisition of intellectual property online, creating and sharing copyrighted material, and fraud and theft of personal information (Holt, 2016). Cyber-porn and obscenity involves a range of deviant and non-deviant sexual expression in the online environment (Holt, 2016). An example of this is the possession and dissemination of Sexually Exploitative Imagery of Children (SEIC), also referred to as child pornography. Cyber-violence encompasses online behaviour that results in physical, psychological, or emotional harm to an individual or groups (Holt,

2016). Acts of cyber-violence include online bullying, harassment and stalking through text messages, social media, and emails.

The increased reliance on technology and the Internet in everyday life has also led to a noticeable increase in cybercrime. The UK fraud prevention service Cifas examined 324,683 fraud cases in 2016 showing an increase of 1.2.% from 2015 (Cifas, 2017). Of these, 53% involved identity fraud, and 88% were facilitated through the Internet (Cifas, 2017). A study released by Javelin Strategy and Research reported that 16 billion US Dollars were stolen from 15.4 million US consumers in 2016, a 17% increase from 2015 (Pascual et al., 2017). A survey of 4,248 US adults found that 41% had experienced online harassing behaviour with different levels of severity, while 66% had witnessed this online abuse being directed at others (Pew Research Center, 2017). The study also found that 18% of the sample had endured severe forms of online abuse including physical threats, sexual harassment and stalking.

As the Internet provided a new venue for criminal activities with an endless supply of potential victims, the virtual world has also witnessed offences committed against youth. A survey of 1,024 young people (aged 11-16) in the UK found that 28% had experienced a distressing event (e.g., bullying, harassment) through their social networking profile (Lilley et al., 2014). The Internet Watch Foundation (2016) identified over 57,000 web pages containing sexually exploitative imagery of children. A survey of 5,700 of students (aged 12-17) in the US found that 34% had experienced different types of online bullying (e.g., hurtful comments, rumours spread), while 12% admitted to the online bullying of others (Samy et al., 2017).

The rapid increase of digital crimes and the use of advanced technologies to commit a diverse range of online criminal acts constantly reinforce the need to develop new standards to deal with digital evidence, and to include other supporting disciplines to assist in Digital Forensics (DF) and digital crime investigations (Casey, 2002, Palmer, 2001). One important approach that could be applied to the DF process and greatly assist in digital crime investigations is Behavioural Analysis (BA), also known as criminal profiling.

1.1 Motivation

This section discusses factors that motivated the research undertaken in this thesis. As described at the beginning of the chapter, the rise in computer-facilitated crimes continues to accelerate causing not only reputational and financial damage to organisations, but also emotional and psychological pain to individuals (Kowalski and Limber, 2013, Staude-Müller et al., 2012). This rise has increased the work load on DF investigators given the limited resources and time constraints, leading to increasing backlogs of evidence awaiting analysis (Karie and Venter, 2015). Further, some types of computer-facilitated crimes (e.g., cyberstalking) present specific

challenges to the DF investigators (e.g., identifying the offender, assessing risk of progression to physical stalking), and despite the severity of the impact it has on the victim, it remains under-prosecuted (Vasiu and Vasiu, 2016).

To overcome some of the challenges presented in DF investigations of such cases, researchers and DF investigators encouraged integrating techniques from other disciplines (e.g., behavioural analysis) within the DF investigation (Bryant, 2016, Rogers, 2003, Wori, 2014). A review of previous work, however, showed that its contribution was through utilising inductive approaches to produce cybercriminal taxonomies. They depended on statistics and generalisation to create an image of the typical offender in specific types of computer-facilitated crimes. This generalised approach, however, is of limited investigative use and does not make practical sense given the uniqueness and specificity of computer-facilitated crimes.

There is also very little research or practice in digital crime investigations that incorporates behavioural and motivational analysis, particularly for computer-facilitated interpersonal crimes. A review of previously developed DF investigation process models showed that their focus was on the technical part of the DF investigation. Two identified DF investigation models that attempted to integrate aspects of behavioural analysis lacked explicit steps to guide the DF investigator on *how* to conduct these steps (see Chapter 2).

Due to the identified factors, the researcher felt the necessity to fill in the gap in the literature by designing a pragmatic DF investigation process model that integrates behavioural analysis and clearly guides the DF investigator into conducting these steps.

1.2 Thesis statement

Behavioural analysis can demonstrate applicability and utility when integrated within the DF investigation process in a post-mortem examination, analysis, and interpretation of the digital evidence of specific types of computer-facilitated crimes.

1.3 Research Aims

This programme of research seeks to build on previous work by scientific researchers and practitioners in developing Digital Forensics Investigation Process Models (DFIPMs). It will focus on an essential part of the investigative phases; the evidence examination, analysis, and interpretation phases. This constitutes the in-lab examination, analysis, and interpretation of the data contained within digital devices associated with the case under investigation. The PhD programme aims to explore the applicability and utility of BA within these phases during the investigation of specific types of computer-facilitated interpersonal crimes. This will expand on previous work by employing a multidisciplinary approach to extend these phases in current

DFIPMs by developing a DF model that incorporates more consideration to aspects of BA. The programme of research addressed this objective by:

1. Examining the usability and applicability of BA in the examination, analysis, and interpretation of digital evidence.
2. Examining the ability of BA to contribute to theoretical understanding of the motivational and behavioural dynamics of computer-facilitated interpersonal crimes.
3. Examining the current use and perceived evidential value of BA in policing and law enforcement.
4. Integrating the findings of the preceding objectives into a usable DF investigation model/tool that incorporates aspects of BA by identifying the phases and sub-phases required to perform the examination, analysis and interpretation of digital evidence for computer-facilitated interpersonal crimes.

Although computer-facilitated crimes include a broad array of online offences (e.g., hacking, malware attacks, and fraud), this thesis will centre on two types of interpersonal cybercrimes: SEIC and cyberstalking. The rationale for selecting these crime categories will be stated in the related study chapters.

1.4 Organisation of the Thesis

This research was organised into three main stages: (1) requirements gathering, (2) design of model, and (3) evaluation of model as shown in Figure 1.1. This section describes the chapters of the thesis, and where these stages fall within them.

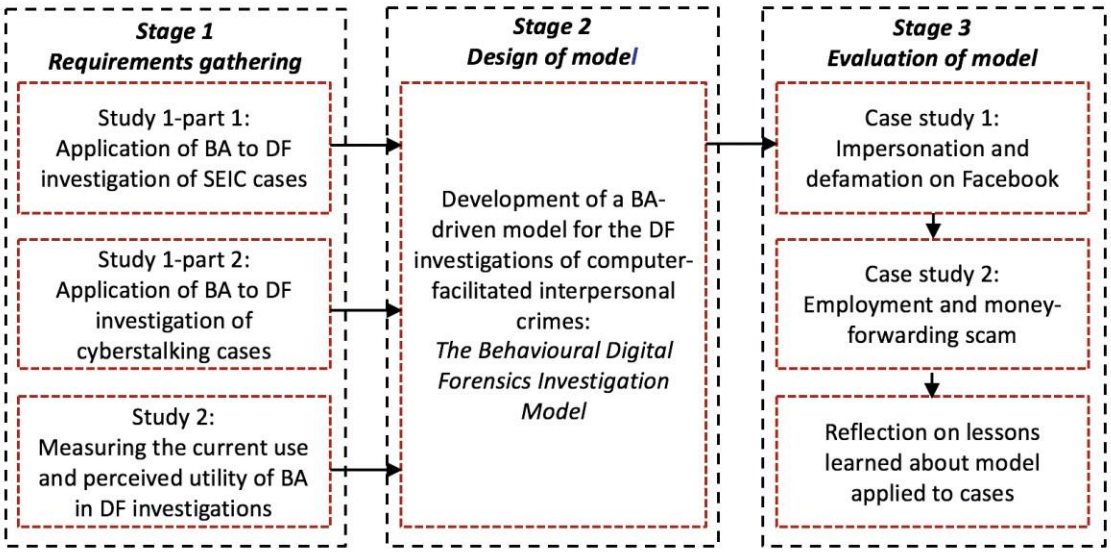


Figure 1.1 Framework of the thesis

This thesis consists of eight chapters, including this one. Chapter 2 presents the review of the literature related to the main aims of the described programme of research (see Section 1.3). The reviewed topics include criminal profiling, DF and its identified challenges, DF investigation models, previous attempts to incorporate BA within DF investigations, SEIC, and cyberstalking. The chapter identifies the limitations in the literature and provides the context for the current programme of research.

Chapter 3 describes and evaluates the methodology used in the programme of research. It highlights the basis of the mixed-methods approach used by providing a critical review of other available approaches. It also includes an examination of different strategies for addressing different research aims, and provides a rationale for the methodological approach adopted for each study conducted.

Chapters 4 and 5 present the first two empirical studies of the first stage of the research framework illustrated in figure 1.1. The studies examined the applicability and utility of BA during the DF investigation process in two types of computer-facilitated interpersonal crimes: SEIC and cyberstalking. It specifically focused on the four strategies of BEA (Turvey, 2011) and identified a number of benefits that each stage of BEA (i.e., equivocal evidence analysis, victimology, crime characteristics, and offender characteristics) contributes to the DF investigation of cases in the selected crime categories. The two studies also examined the characteristics, behaviours, and motivations of SEIC and cyberstalking offenders, and compared this to the currently available relevant research evidence. Exploring the ways in which BA can be integrated within the DF investigation process of the SEIC and cyberstalking sample cases provided an insight into the extent and limits to which BA can be utilised. Along with the review of process models which incorporate BA, reviewed in Chapter 2, this helped identify the necessary structure to design a model that will aid DF investigators to perform each step of the examination, analysis, and interpretation of digital evidence to achieve reliable results

Chapter 6 presents the results of an online survey study (Stage 1 in Figure 1.1) empirically examining the perceptions of national and international digital forensics investigators regarding the use and utility of BA during the process of investigating SEIC and cyberstalking cases. The results indicated that while the majority of participants indicated that BA has the potential to contribute to many aspects of DF investigations, their daily investigative activities involved a limited use of this technique. The implications of the study were examined, and emphasised the need to design a DF model that provides guiding steps and illustrations of how to utilise BA in DF investigations.

Based on results from the conducted studies (Stage 1 in Figure 1.1), a DF investigation model that incorporates aspects of BA was developed in Chapter 7 (Stage 2 in Figure 1.1). It aimed to provide a practical, structured, multidisciplinary approach to performing a post-mortem examination, analysis, and interpretation of the content of the digital devices associated with computer-facilitated interpersonal crimes. Two case studies were used to evaluate and illustrate the usability of the model in investigating computer-facilitated interpersonal crimes (Stage 3 in Figure 1.1). Two real digital crime cases were obtained from Dubai police and the researcher used the phases and sub-phases of the developed model and described how each of them was conducted in relation to investigating the cases. A case study strategy was employed to provide a descriptive, in-depth analysis of the case, and provide a clear step by step guide on how to apply the different phases and sub-phases of the model. Also part of Stage 3 (Figure 1), was a reflection of lessons learned in terms of: (1) how the application of the model contributed to the investigation of the case, and (2) how the results of the conducted examination with the proposed model compared to results from the original cases report.

Finally, chapter 8 provides a general discussion of the findings and conclusions.

2 LITERATURE REVIEW

2.1 Introduction

This chapter presents the literature review and it is organised as follows. Section 2.2 provides an overview of criminal profiling. It covers the definition of criminal profiling and the history of its evolution. Further, it critically reviews and evaluates previous criminal profiling approaches, including the FBI's typology and Investigative Psychology. It then introduces the general term of Behavioural Analysis (BA), and the sub-set Behavioural Evidence Analysis (BEA) (Turvey, 2011), including its strategies and principles, and argues that it is a more effective practical alternative for investigating computer-facilitated crimes than the previously described approaches.

Section 2.3 provides a brief overview of Digital Forensics (DF) and its identified challenges, while section 2.4 focuses on Digital Forensics Investigation Process Models (DFIPMs). It details the development and structure of thirteen DFIPMs developed by investigators and academics, which have been developed between 2001 and 2016. It identifies the limitations of each model, as well as the broader general limitation of not considering the human behavioural and motivational factors that have relevance for identifying potential evidence during the investigation process.

Section 2.5 discusses incorporating BA within the digital forensics investigation process. It identifies two published research studies that have attempted to integrate aspects of BA within the DFIPM: (1) Digital Forensics Profiling Methodology for Cyberstalkers (Silde and Angelopoulou, 2014), and (2) Roger's Behavioural Analysis Model (Rogers, 2015). The section provides a comprehensive review of these models and identifies their limitations. It confirms the recent consideration of researchers of the utility of BA in digital forensics investigations, and

the limitations of the literature in providing pragmatic, clearly described DFIPMs that incorporate BA.

Section 2.6 provides an overview of the literature on the online possession and dissemination of Sexually Exploitative Imagery of Children (SEIC), one of the categories of crime addressed by the programme of research. It focuses on offender characteristics, offender typologies and motivation theories, and victim characteristics. Section 2.7 provides an overview of the cyberstalking literature, with specific focus on forms of cyberstalking, offender characteristics, offender typologies and motivation theories, and victim characteristics.

2.2 Criminal Profiling

Criminal profiling is a forensic technique used in criminal investigation for analysing, assessing, and interpreting the physical evidence, the crime scene, the nature of the offence, and the way it was committed (Ainsworth, 2013, Douglas et al., 1986, Kocsis, 2006). This aims to create a profile of the demographic and behavioural characteristics of an offender against the characteristics of those who have previously committed similar crimes (Kirwan, 2011, Kocsis, 2006). A criminal profile may include physical (e.g., gender, age, background, height), and behavioural and psychological attributes (e.g., psychological disorders, guilt, anger) (Ainsworth, 2013, Kocsis, 2006). Criminal profiling does not necessarily identify a specific offender. However, it effectively narrows down the pool of potential suspects and enables a more efficient use of investigative resources (Douglas et al., 1986, Ferguson, 2014). Criminal profiling uses three broad forms of inferential reasoning for creating a subject profile: induction, deduction, and abduction. Sections 2.2.1-2.2.3 provide an overview of each.

2.2.1 Inductive Reasoning

Inductive reasoning utilises statistical analysis of behavioural and psychological data from convicted criminals (Turvey, 1998, Warikoo, 2014). It relies on data from criminal databases to identify a generalised behavioural pattern and personality traits of a typical offender in specific types of cases (e.g., rape, serial murder) (Rogers, 2003, Warikoo, 2014). After identifying a behavioural pattern or specific characteristics of a typical offender, the investigator can use criminal databases or records related to the defined characteristics to develop a group of potential suspects (Rogers, 2003).

2.2.2 Deductive Reasoning

Deductive profiling relates to case-based investigations. It analyses evidence from the case in question focusing on specific behavioural and personality traits, and uses it to develop a profile of the specific characteristics of the probable offender (Turvey, 2011, Warikoo, 2014). It avoids

generalisations and averages and depends on processing information on all of the available instances of a crime. As such, it is based on a scientific forensic assessments of a crime's variables and attributes that require specialised forensic and psychological skills (Holmes and Holmes, 2009, Turvey, 1998).

2.2.3 Abductive Reasoning

Abductive reasoning involves making inferences to the best explanation using the available evidence (Carson, 2009). It starts with an incomplete set of evidence/observations and tries to construct the most likely explanations, draw conclusions, or make predictions out of this set (Fahsing and Ask, 2018). Abduction has been linked to the investigative skills of Sherlock Holmes, and is claimed to provide a better inferential reasoning in terms of the generation and evaluation of hypotheses based on the available evidence (Carson, 2009, Fahsing and Ask, 2018). With regards to reconstructing the crime events, it has been suggested that abduction aids in producing a better interpretation of the events surrounding the crime by focusing on the essential evidence and discarding irrelevant information (Carson, 2009).

The benefits of abductive reasoning, however, does not make induction and deduction less important. In a real criminal investigation, the three techniques can be used to complement each other to uncover evidence and illuminate the truth.

2.2.4 History of Criminal Profiling

The field of criminal profiling is conceptually old. Understanding the enemy is an approach that has been used in military and business strategy for hundreds of years (Tzu, 2013). In the 19th century, the role of criminal profiling in criminal investigation started to gain more attention when Dr Thomas Bond performed a deductive criminal profiling on the serial killer Jack the Ripper (Canter, 2010). He performed an autopsy on the last victim of the killer in an attempt to reconstruct the crime and interpret the behavioural patterns of the offender (Alison, 2013, Canter, 2010). After the examination and analysis, he constructed a profile that included the possible physical and personality traits of the offender (Keppel et al., 2005, Miller, 2014). The Jack the Ripper case was never solved; however, since this case criminal profiling has continued to develop and aided in the investigation of a variety of crime categories (e.g., murder, rape, sexual assault) (Geberth and Bagerth, 1996, Holmes and Holmes, 2009).

In the 1970s, FBI agents of the Behavioural Science Unit proposed that behavioural analysis of crime scenes can assist in constructing profiles of offender characteristics (Ressler et al., 1988). They claimed that the behavioural characteristics of the offender could be inferred from the examination of a crime scene, as it reflects distinctive aspects of their personality (Douglas et al., 2013, Douglas et al., 1986, Ressler et al., 1988). Based on reviews of case records, and

investigative interviews with 36 offenders, they characterised offenders into two groups: organised and disorganised. The crime scene related to an organised offender is claimed to reflect a level of planning, control, and sophistication (Douglas et al., 2013, Douglas et al., 1986). For example, the offender uses different locations to commit the crime. The victim is abducted from one location, and moved to another where the crime is committed. The victim's body is then disposed of in a third location. Restraining tools (e.g., rope, adhesive tape) are used to control the victim. The offender tampers with the evidence and uses measures to conceal evidence (e.g., removing the murder weapon from the crime scene, eliminating fingerprints). In contrast, the crime scene of a disorganised offender will be chaotic and reflect a sense of disorder (Douglas et al., 2013, Douglas et al., 1986). For example, the offender fails and/or does not make an effort to cover evidence (e.g., blood, fingerprints, murder weapon). The victim's body is left in open view, and clothing are scattered on the crime scene.

Despite the wide acceptance and use of the FBI model, it has been criticised for not providing detailed information of the underlying theoretical concepts (Canter et al., 2004, Kocsis and Palermo, 2016). It was also criticised for the small, unrepresentative sample used to develop the model, the use of unstructured interview procedures, and failure to provide a clear methodology for how the model was constructed (Canter et al., 2004, Higgs et al., 2017). Also, depending only on offender behaviours reflected in the crime scene is not sufficient (in every crime) to place them in one of those categories (Canter et al., 2004, Van Aken, 2015). The model also does not consider the potential relationship between victims and offenders, which can lead to misclassification of offenders (Van Aken, 2015). Finally, analysing the data of 100 serial killer crimes in another study indicated that the majority of offenders exhibited behaviours that placed them within the organised offender category (Canter et al., 2004). This could indicate that the disorganised category is not empirically valid.

In 1992, David Canter developed a framework known as Investigative Psychology (Canter and Youngs, 2009). This framework used an inductive approach to ensure a grounding in scientific methodology. It involved analysing crime scenes, and other subsets of crime information for the behavioural characteristics of unknown offenders in previously committed crimes, and comparing these traits to ongoing crime investigations (Snook et al., 2008). This approach, however, was criticised on the basis that statistical analysis cannot by itself be sufficient in predicting future behaviour (Copson et al., 1997). For example, offenders with similar characteristics will not necessarily commit similar crimes in a similar way (Alison et al., 2002). Therefore, inferences drawn from statistical analysis are not guaranteed to be completely valid for all offenders in similar crime categories.

Both the FBI's typology and the Investigative Psychology approach were developed based on generalisation and statistical analysis, which make them of limited use in real criminal

investigations (Rogers, 2003). This is because offenders with similar characteristics do not necessarily behave in a similar manner when committing crimes, have similar motivations, or depend on a unified *Modus Operandi* (MO) to commit similar offences (Wori, 2014). In an attempt to overcome some of the limitations of the FBI typology and the Investigative Psychology approach, Turvey (2011) developed the Behavioural Evidence Analysis model (BEA). It is a deductive-based forensic technique that uses the evidence in a case to understand and reconstruct the behaviour of the criminal. This model consists of four stages: equivocal forensic analysis, victimology, identification of crime scene characteristics, and identification of offender characteristics (Turvey, 2011). These stages are described in Section 2.2.6.

2.2.5 Behavioural Analysis (BA)

Criminal profiling has been referred to, among other less common terms, as behavioural analysis, behavioural profiling, crime scene profiling, offender profiling, psychological profiling, investigative profiling, and criminal investigative analysis (Annon, 1995, Hazelwood et al., 1995, Palermo and Kocsis, 2005, Rogers, 2003, Rogers, 2015). Due to the lack of uniformity in the use of the terms, as well as the interchangeable and inconsistent application, for the purpose of the research, the term Behavioural Analysis (BA) will be used and is considered a general technique to performing criminal profiling. BEA, described in the next section, is considered as a subset of BA. Figure 2.1 shows the relation between the three frameworks.

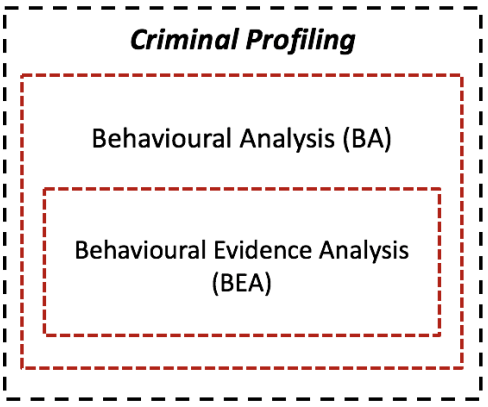


Figure 2.1 Subsets of criminal profiling

2.2.6 Behavioural Evidence Analysis (BEA)

BEA (a subset of BA) is a deductive, case-based investigative strategy that analyses evidence from a specific case focusing on certain behavioural and personality traits to derive the characteristics of the probable offender (Turvey, 2011). This section describes the four strategies that constitute BEA, as well as the principles on which it is based.

2.2.6.1 Equivocal Forensic Analysis

According to Casey et al. (2014), an equivocal forensic analysis refers to the process of conducting a scientific assessment of the case evidence that includes:

1. A thorough examination, analysis, and evaluation of evidence, employing critical thinking, reasoning, and logical analysis. For example, in a computer-facilitated interpersonal crime where the investigator receives the victim's computer, the investigator should not only analyse the content of the subject files (e.g., emails, chat messages, blogs), but they should also pay attention to the meta-data related to these files, as well as other data informative to the case. Timestamps and IP addresses retrieved from emails can reveal information about the offender. Recovering and reconstructing artefacts left by the use of instant messaging tools (e.g., Facebook chat) can reveal information regarding the chat message such as the unique message ID, the sender's name and profile number, the recipient's name and profile number, and the date and time the message was sent (Al Mutawa et al., 2011). Collecting this data and analysing them in a logical way can enable the linking of pieces of information, and reconstruct the timing of events in order to help the investigator develop a better understanding of the case.
2. A consideration of all the possible interpretations of the evidence. Since evidence can often be interpreted in more than one way, it is very important to be aware of all these possible interpretations in order to determine the most probable meaning of the collected data.
3. A critical and careful assessment of all assumptions and conclusions made by other parties investigating the case.

This strategy aims at reviewing the case evidence thoroughly and objectively to develop theories that are justified by the actual facts, to avoid confusion in an investigation, and to gradually illuminate the truth.

2.2.6.2 Victimology

Victimology refers to the study of victims in criminal investigations and explaining the opportunities for victimisation (Karmen, 2012). It involves a thorough scientific study of a victim's characteristics, daily routines, and lifestyle behaviour that may have contributed to their selection (Casey et al., 2014, Karmen, 2012). This strategy aims to identify why/how/when/where the particular victim was targeted and/or approached. It also examines information about the victim, including physical traits, marital status, personal lifestyle, occupation, education, last known activities, friends and enemies, and personal diaries. This

assessment of the victim can provide indications of the offender's motive, and their connection to the victim. It can also provide investigative direction in a case to other potential sources of digital evidence that could have been overlooked (Turvey, 2014). The development of an analysis of the victimology associated with a specific crime has also been identified as important as it enables investigators to develop a clearer understanding of the selection of a specific victim, and identify evidence linking victims and offenders (Casey et al., 2014, Turvey, 2011).

2.2.6.3 Crime Scene Characteristics

The digital world allows offenders to be in different physical locations than their victims or even use multiple locations to confuse investigators and avoid detection (Turvey, 2011). They may also use specific virtual locations in cyberspace that match their motivations and planned offences (e.g., online grooming of children). For example, online sex offenders can use specific chat rooms or social networks that attract underage individuals to select targets, or meet with other criminals whom live within the same physical area. The characteristics of the virtual crime scene that the offender chooses can provide investigators with information about the offender and their motivation (Casey et al., 2014, Turvey, 2011). For example, an offender that is motivated by monetary gain can use malicious software to gain remote access to the victim's computer (e.g., a company). Once remote access is established, extortion may be used to make the company pay the offender in return for not deleting important data. A careful examination of the unique characteristics of the digital crime scene can also answer questions regarding the case, uncover more evidence, and correlate with the offender's behavioural decisions (Turvey, 2011).

2.2.6.4 Offender Characteristics

The final step is analysing offender characteristics. Combining the three preceding BEA strategies during a digital crime investigation can help determine the probable behavioural and personality characteristics of the offender. For example, victimology can reveal information about the motivations for targeting a specific victim. Whether it was opportunistic, or that the offender had intended to victimise a specific individual in particular (e.g., selecting a victim within a specific local area). Evidence of a previous relationship with the victim can reduce the suspect pool to those known to the victim. It can also indicate the motivation for offending (e.g., acting on anger after the victim ended a relationship). The use of specific tools to commit the crime can indicate the MO of the offender. Evidence of measures to evade detection and hide the offender's online behaviour provides an indication of their technical sophistication level. Thus, the choices made for targeting a victim, the methods used to commit the offence, and other evidence extracted from the previous stages provide indications of the behavioural traits of the probable offender (Turvey, 2011).

2.2.6.5 The principles of Behavioural Evidence Analysis

As with any field of study, BEA is based on the basic principles identified by Turvey (2011), which were derived from biological and behavioural sciences. The principles can be summarised, but not limited, to the following:

1. *The principle of uniqueness.* There are no two identical cases. Each case is unique to itself even though it may have similarities with others.
2. *The principle of separation.* The digital investigator should be objective while investigating and analysing the evidence, and separate their personal feelings from interfering with the interpretation of the evidence.
3. *The principle of behavioural dynamics.* An individual's behaviour is dynamic. It could change, evolve, or devolve over time resulting in the reflection of different behavioural characteristics even when committing similar crimes.
4. *The principle of behavioural motivation.* All behaviour results from underlying motives, whether these motives were conscious or subconscious.
5. *The principle of multidetermination.* A single behaviour can result from multiple purposes.
6. *The principle of behavioural variance.* Similar offences may be committed for completely different motives.
7. *The principle of reliability.* Conclusions from a digital forensic examination and analysis must be reliably established based on facts derived from concrete evidence and reasoning.

2.2.7 The Role of Behavioural Analysis in Investigating Digital Crimes

A number of studies have emphasised the effective role of BA in assisting in conventional criminal investigations (e.g., murder, sex offences) (Beauregard et al., 2017, Bennett and Hess, 2007, Lowe, 2002, Tonkin et al., 2017). Tonkin et al. (2017) applied different statistical methods to analyse crime scene behaviours of offenders in a dataset of 3,364 solved and unsolved serial sexual assaults committed in five countries. They found that distinguishable offender behavioural patterns (e.g., method of approach, level of violence used, method used to restrain the victim) could be identified, and had a significant level of accuracy in linking sexual offences committed by the same offender. Beauregard et al. (2017) recognised that the behavioural profiling of offenders and victims (victimology) is invaluable for investigative interviewing. They surveyed 624 incarcerated sex offenders and analysed case-related documents to develop behavioural profiles of them and their victims. They generated five profiles for offenders and five profiles for victims depending on their likelihood of confession

during an interrogation. Based on their findings, possible interrogation strategies were designed for each profile to aid in obtaining confessions.

Rogers (2003) argued that BA can be of equal effectiveness in assisting in the investigation of digital crimes. Similar to offenders of crimes committed in the physical space, offenders committing a similar type of cybercrime (e.g., online harassment) can be driven by different motivations and intentions. Also, the general set of investigative questions (e.g., what motivated the offender, why the offender selected a specific victim) that need to be answered to understand the events of a digital crime are the same as they would be for investigating a conventional crime (Wori, 2014). Bryant (2016) argued that a careful application of criminology in the investigation of digital crimes can provide investigators with additional leads and direction.

As such, to efficiently solve a digital crime, it is important to learn as much as possible about the individual behind the offence, as well as the victim (Canter and Youngs, 2009, Wori, 2014). The DF investigators need to employ more than technical examinations of the digital evidence as technology by itself is inadequate to solve the problem. It is important to understand the motivation and the unique behavioural characteristics of the offender in order to effectively investigate digital cases of deviant computer behaviour (Turvey, 2011). For example, the behaviour of offenders and risk of engaging in violent acts (e.g., mass murder, school shootings) can be identified from their written or spoken language (e.g., written communication, threats, or notes made by the offender) (Kaati et al., 2016). The analysis of this data can provide the investigators with a wealth of information (e.g., the motivation behind the offence, the relationship to the victim) (Smith and Shuy, 2002). The use of specific words and the tone of the language can reveal the psychological state of the offender (e.g., anger, revenge, greed) (Douglas et al., 1986, Kaati et al., 2016). Analysing files of their computer (e.g., Internet history files, recently accessed files, access dates of the files, deleted files) can reveal indicators of suspicious activity, as well as signature behaviour and personalised characteristics of the offender (Rogers, 2003). This information helps the investigator to develop leads, and determine the location of additional sources of evidence (Turvey, 2011).

After identifying all the supporting evidence in a case, the investigators can create a more solid reconstruction of the crime that aids in understanding what happened, and provides an explainable basis for expert judgment and opinion. To accomplish this crucial task in an investigation, the investigators must focus on BA including the four basic case assessment strategies of BEA described in Section 2.2.6.

2.3 Digital Forensics

Digital forensics, also known as computer forensics and forensic computing, is a branch of forensic science that denotes the processes of uncovering, analysing, and interpreting electronic data stored on digital devices during the course of a criminal investigation (Casey, 2002, Casey et al., 2014). It is usually performed in incidents where a digital device was used to commit a crime, as a tool to facilitate a crime, or as storage to evidence connected to the crime. Despite the difference in the nature of evidence used, the goal of the DF investigation is similar to that of a conventional criminal investigation, which is to identify the party responsible for committing the crime (Casey, 2002, Casey et al., 2014).

Similar to the investigative methods used in a conventional crime, digital forensics incorporates the use of scientifically proven methods for the identification, preservation, collection, validation, analysis, interpretation, documentation, and presentation of digital evidence stored on or transmitted by electronic devices used to commit or facilitate a crime (Ademu et al., 2011). Recovered evidence can facilitate the reconstruction of a criminal event, assist in incriminating or exonerating suspects, and support the prosecution of different types of crimes (Cohen, 2013). Electronic evidence must be recovered in a forensically sound manner in order for it to be admissible in a court of law (Casey, 2002, Casey et al., 2014). The DF investigator must preserve the integrity of the original digital evidence and prevent any alteration, contamination, or destruction of it. This entails the development and use of formal procedures and policies that ensures the proper handling of digital evidence (Casey, 2002, Casey et al., 2014). Thus, the DF investigator must ensure the integrity of the methods and procedures applied during an investigation in order to assure the credibility and efficiency of the recovered evidence in supporting the prosecution of a digital crime.

2.3.1 Challenges in Digital Forensic Investigations

The dramatic evolution of technology has consequently resulted in an increase in the techniques, sophistication, complexity and number of cybercrimes (Lillis et al., 2016). This has resulted in the continuous emergence of a variety of challenges to be faced in the DF domain (Vincze, 2016). A long list of DF challenges have been identified in the literature (Franke et al., 2017, Lillis et al., 2016, Samy et al., 2017, Vincze, 2016). Karie and Venter (2015) reviewed the DF challenges identified by researchers and academics during the last ten years, classifying them into four distinguished categories: (1) technical challenges, (2) legal systems and/or law enforcement challenges, (3) personnel-related challenges, and (4) operational challenges. The technical challenges included twelve sub-categories which were encryption, vast volumes of data, incompatibility among heterogeneous forensic tools, volatility of digital evidence, bandwidth restrictions, limited life span of digital media, sophistication of digital crimes,

emerging technologies and devices, limited window of opportunity to collection of potential digital evidence, anti-forensics, acquisition of information from small-scale technological devices, and cloud computing. These challenges were related to those that can be tackled with existing expertise, protocols, and operations (Karie and Venter, 2015).

Legal systems and/or law enforcement challenges refer to those that can affect the successful prosecution of a digital crime (Karie and Venter, 2015). This included jurisdiction, the legal process of prosecuting digital crimes, admissibility of DF tools and techniques, insufficient support for legal criminal or civil prosecution, ethical issues, and privacy. The personnel-related challenges included the lack of qualified DF personnel (e.g., training, education, and certification), semantic disparities in digital forensics, lack of unified formal representation of DF domain knowledge, lack of forensic knowledge reuse among personnel, and forensic investigator licensing requirements. The operational challenges included incidence detection, response and prevention, lack of standardised process and procedures, significant manual intervention and analysis, DF readiness in organisations, and trust of audit trails. This may imply that conventional methods for investigating digital crimes are no longer practical, and new methods and approaches must be developed to overcome these challenges.

2.4 Digital Forensics Investigation Models

As DF is a fairly new discipline compared to other forensic science fields, continuous efforts are taking place to develop methods and standards to provide a standardised and structured digital forensics investigation process. As mentioned in the previous section, lack of standardisation was identified as one of the major challenges for the DF domain. The lack of standardisation, and the discrepancies between the available models hinders the DF process, and can result in incomplete evidence collection, errors in interpretation, and restrict admissibility in court (Du et al., 2017, Karie and Venter, 2015). A standardised DFIPM will enhance the scientific rigor of the process, facilitate applicability and further research (Beebe and Clark, 2005). The need for a standard model for digital forensics was initially raised during the first Digital Forensics Research Workshop (Palmer, 2001). Since then, scientific researchers and practitioners have made a number of attempts to develop a standard DFIPM. This section details the development and structure of a number of DFIPMs highlighted in the field by practitioners and academics. It also provides an examination of how they differ and a critique of each of them.

2.4.1 Electronic Crime Scene Investigation Model

The U.S. Department of Justice developed a DFIPM for electronic crime scene investigation which consisted of guidelines for first responders (Holder et al., 2001). It included four phases: (1) securing and evaluating the scene, (2) documenting the scene, (3) evidence collection, (4)

packaging, transportation, and packaging of digital evidence. It also referenced the different types of electronic evidence and described the proper methods to handle them. The guide's main emphasis was on the collection and handling of digital devices/evidence being oriented towards first responders to a physical crime scene. Whilst this guide focused on an essential phase of the DF investigation process, it paid little attention to other important phases such as the examination and analysis processes. Also, while it provided a chapter on digital evidence consideration by crime category, the only focus was on digital devices where potential evidence might be found for each crime category. It basically included lists of digital devices to be seized during the investigation of specific crime categories. As such, the guide provided basic technical information on digital devices and data collection at crime scenes, but did not consider any behavioural analysis of the available information to assist in crime reconstruction or offender apprehension.

2.4.2 An Abstract Digital Forensics Model

Reith, Carr and Gunch (2002) argued that existing DFIPMs were not standardised and were overly specific to certain technologies. They proposed an abstract DFIPM which used a generalised methodology that was not specific for a certain technology or type of digital crime. Their model included nine steps: (1) identification, (2) preparation, (3) approach strategy, (4) preservation, (5) collection, (6) examination, (7) analysis, (8) presentation, and (9) returning evidence. Their proposed model, however, was too general for practical use and there was no easy method for its testing and validation (Reith, Carr, & Gunch, 2002). The model also does not provide a clear line between the *preparation* and the *approach strategy* phases, as they appear to overlap.

2.4.3 An Integrated Digital Investigation Process

Carrier and Spafford (2003) proposed the Integrated Digital Investigation Process (IDIP) which combined physical and digital crime scene investigation. Their model included five groups with a total of 17 phases: (1) readiness, (2) deployment, (3) physical crime scene investigation, (4) digital crime scene investigation, and (5) review. Unlike previous process models, the IDIP emphasised the importance of the physical crime scene in digital crimes. It provided an equal number of phases for the physical and the digital crime scenes, and considered them to be a primary and a secondary crime scene respectively. It also included detailed descriptions of what each phase constituted. The authors provided two case studies to illustrate the activities required in the phases described in the model. The case studies, however, were not performed on real cases. The authors used common scenarios based on their experiences to illustrate application of the model. The provided information was of high-level description and did not include comprehensive details of the investigation. Another drawback, despite being based on the crime

scene theory for physical investigations, was that the model did not consider other traditional investigative approaches, for example, using the gathered information to create an initial profile of the offender.

2.4.4 Enhanced Digital Investigation Process

Baryamureeba and Tushabe (2004) proposed the Enhanced Digital Investigation Process Model, a modification of the IDIP model. The model aimed at avoiding reconstruction inconsistencies by separating the investigation into two crime scenes: the primary crime scene (computer) and the physical crime scene (the actual physical crime scene). It included five phases: (1) readiness, (2) deployment, (3) trace back, (4) dynamite, and (5) review. The phases of the model were briefly described and no detailed information was provided as to how these phases should be used in the evaluation of a crime scene. Also, no attempts were made to illustrate the use of the model in real cases. Finally, Mir et al. (2016) criticised this model to be limited to digital-fraud crimes.

2.4.5 A Hierarchical Objective Based Framework for the Digital Investigations Process

Beebe and Clark (2005) proposed the hierarchical, objective-based framework for the digital investigation process which had the novel approach of being multi-tiered. Their model provided the level of detail needed for practicality and specificity. They compared previous work on the subject to their work and mapped phases of previous DFIPMs to the first tier of their proposed model. Their aim was to combine the achievements of previous models to create synergy between these different perspectives. The first-tier included six phases: (1) preparation, (2) incident response, (3) data collection, (4) data analysis, (5) presentation of findings, and (6) incident closure. In their second-tier phases (sub-phases), they specified that all types of crime and digital evidence should be included, with related task hierarchies subordinate to specific objectives. Their study, however, mainly focused on providing detail on the application of the model to the *data analysis* phase. As noted by the authors, other phases required extension through further research to include details of their sub-phases. They also provided two case studies to demonstrate how the phases and principles of the model could be applied to DF investigations. The case studies, however, were not based on real cases, but on fictional scenarios.

2.4.6 Digital Forensic Model Based on Malaysian Investigation Process

Perumal (2009) reviewed 13 preceding DFIPMs and criticised them for having shifting focuses, with each focusing on a specific aspect of the DF investigation (e.g., data analysis). He also claimed that previous models lack the presentation of information process flow (e.g., chain of

custody), and paid little attention to data acquisition and handling of fragile evidence. He proposed the Digital Forensic Model based on the Malaysian Investigation Process, which was a model claimed to capture the full scope of an investigation process (Perumal, 2009). It included seven phases: (1) planning, (2) identification, (3) reconnaissance, (4) analysis, (5) results, (6) proof and defense, and (7) diffusion of information. Although claimed to focus on the full scope of the investigation, the model seems to mainly focus on data acquisition for different types of digital evidence (e.g., static data, live data). It provides a brief description of the other phases and does not provide examples to illustrate how the phases are applied to the investigation of real cases.

2.4.7 Cohen's Digital Forensics Process Model

Further research resulted in a DFIPM that addressed the challenges and legal issues concerning digital evidence (Cohen, 2010). This model focused on the principal elements of the DF examination phase, including analysis, interpretation, attribution and reconstruction. The phases are explained in a general and comprehensive form; however, no illustrations were provided to demonstrate how to pragmatically implement them in real cases.

2.4.8 The Systematic Digital Forensic Investigation Model

Agarwal et al. (2011) proposed the Systematic Digital Forensic Investigation Model. Their model included eleven phases: (1) preparation, (2) securing the scene, (3) survey and recognition, (4) documentation of the scene, (5) communication shielding, (6) evidence collection, (7) preservation, (8) examination, (9) analysis, (10) presentation, and (11) result. The authors provided detailed description of each phase including their objectives and required actions. The model generally explained the handling of static and volatile data. It explored the different processes required in the investigation of cases involving computer fraud and cybercrime in order to aid investigators and organisations to define appropriate policies and procedures (Ademu et al., 2011). The model, however, was oriented towards the investigation of computer fraud and cybercrimes only, which may limit its applicability to other categories of computer-facilitated crimes.

2.4.9 A New Approach for Digital Forensic Investigation

In an attempt to design a simplified iterative DFIPM, Ademu et al. (2011) proposed a four-tier iterative model that included: (1) preparation, (2) interaction, (3) reconstruction, and (4) presentation. Each of the phases included sub-phases. For example, the preparation phase included preparation, identification, authorisation, and communication. The model was derived and structured from preceding models. The authors, however, do not provide any description of

the model phases and sub-phases. Also, the model has not been tested on real cases (Mir et al., 2016).

2.4.10 Harmonised Digital Forensic Investigation Process Model

Valjarevic and Venter (2012) proposed a generic DFIPM that aimed at harmonising existing models. It is an iterative and multi-tiered model that comprised twelve phases: (1) incident detection, (2) first response, (3) planning, (4) preparation, (5) incident scene documentation, (6) potential evidence identification, (7) potential evidence collection, (8) potential evidence transportation, (9) potential evidence storage, (10) potential evidence analysis, (11) presentation, and (12) conclusion. The model used parallel actions in implementing the DF process. This refers to including actions that must be performed in parallel with each phase (e.g., documentation, preserving the chain of evidence). The authors argued that these parallel actions were needed to achieve higher efficiency of the investigation, and admissibility in court. Similar to previous DFIPMs, this model has not been tested on real cases.

2.4.11 Integrated Digital Forensic Process Model

Kohn et al. (2013) analysed six existing DFIPMs and used them to propose an integrated model with purified terminology. The model constituted phases and sub-phases where the phases include: (1) preparation, (2) incident, (3) incident response, (4) physical investigation, (5) digital forensics investigation, and (6) presentation. To maintain the chain of custody, the authors identified documentation as a continuous process that must be performed throughout the phases of the investigation. A comprehensive account was offered for each phase, yet the sub-phases were not explicitly and clearly described. Also, the model seemed to be oriented toward organisational incidents, which limits its applicability to other categories of digital crimes.

2.4.12 Integrated Computer Forensic Investigation Process Model for Computer Crime Investigation

Montasari et al. (2015) argued that previous DFIPMs fail to address the practical requirement of DF investigators, and do not sufficiently describe all these model's associated phases. They proposed a model that included eight phases: (1) readiness, (2) identification, (3) incident response, (4) collection, (5) examination, (6) analysis, (7) presentation, and (8) incident closure. Although the authors claimed to integrate phases, sub-phases, principles, and objectives into their model, only high-level representation of the model was offered. Their paper was limited to short descriptions of each phase. The authors stated that further research would be conducted to extend the model and provide a comprehensive account of sub-phases, procedures, and guidelines. As such, their current model offers very little information to be of practical use to DF investigators.

2.4.13 Mir's et al. (2016) Digital Forensics Process Model

Mir et al. (2016) reviewed previous DFIPMs and proposed a framework that was based on the models designed by Perumal (2009) and Cohen (2010). They argued that earlier models have limited scope in focusing on one aspect at a time (e.g., volatile data). They claimed that their proposed model addressed this limitation by having a wider scope covering three aspects of the DF investigation process: (1) data acquisition, (2) fragile evidence, and (3) examination. Their model included ten phases: (1) planning, (2) identification, (3) collection, (4) reconnaissance, (5) transport and storage, (6) examination, (7) analysis, (8) proof and defence, (9) archive storage, and (10) presentation and results. The model was presented as a diagram that included high-level phases of the DF investigation process. The authors did not offer any information about what each phase constituted, nor on how the previously mentioned three aspects of the DF investigation process were addressed. There was no indication of any iterative processes between the phases, which is essential in the investigation of digital crimes (e.g., analysis of digital evidence can lead to the identification of further digital devices). Finally, the model was not tested for its practicality, nor was there an illustration on how to apply it when investigating a digital crime.

2.4.14 General Limitations in Earlier Models

Whilst various DFIPMs have been proposed, developed and refined during the past years, none of them have been formally standardised. Most of the previously proposed DFIPMs were single-tier process models that focused on the higher levels of the investigation process without providing enough detail about the principles of the investigation. Several authors of these models have suggested that additional specific steps within each phase (e.g., providing clearer definitions of what the phase constitutes, identifying the objective of each phase, providing guiding steps on how to conduct each phase) are needed to provide adequate detail in order to be useful to the DF investigator (Carrier and Spafford, 2003, Mir et al., 2016, Montasari et al., 2015, Palmer, 2001, Reith et al., 2002).

None of the preceding DFIPMs indicated that they had been empirically tested on real cases. They also lacked empirical testing pertaining to the theories and techniques associated with their production. Models that provided an illustration on their application used fictional case scenarios and provided limited information that did not clearly show how their phases were utilised. Also, models that provided details about these different phases focused on *what* must be conducted during each phase, but failed to provide sufficient guidance on *how* to conduct the investigation. Greater detail on the phases and sub-phases, goals, and procedures in these models is needed in order to improve their usability for DF investigators and researchers alike.

Also, the previous DFIPMs usually disregard the human element in a DF investigation and do not consider the behavioural, motivational or social dimensions of criminal behaviour that have relevance for identifying potential evidence during the investigation process. This review of available models suggests that authors have mainly focused on the technical aspects of the DF investigation process (e.g., data acquisition, preserving volatile data). Finally, the proposed models lack verification and validation methodologies.

2.5 Integrating Behavioural Analysis in Digital Forensics Investigation Models

Up until 2014 there were no DFIPM that acknowledged the utility of including aspects of BA within the DF investigation process. However, researchers have recently started to recognise the importance of integrating other disciplines within the DF investigation process, as was evident in their attempts to produce DFIPMs that incorporated aspects of BA (Rogers, 2015, Silde and Angelopoulou, 2014). There is, however, very little research or practice in digital crime investigations which incorporates BA. There is even less in the literature that concerns the utility of BA in interpreting the digital evidence in these crimes.

There have been two published research that have attempted to incorporate BA within the DF investigation of interpersonal crimes, specifically the possession and dissemination of Sexually Exploitative Imagery of Children (SEIC) and cyberstalking crimes: (1) Digital Forensics Profiling Methodology for Cyberstalkers (Silde and Angelopoulou, 2014), and (2) Roger's Behavioural Analysis Model (Rogers, 2015). The remainder of this section will review these models.

2.5.1 Digital Forensics Profiling Methodology for Cyberstalkers

Silde and Angelopoulou (2014) developed a cyberstalker profiling methodology by incorporating elements from BEA (a subset of BA) into a standard digital forensics investigation framework. Their model constituted three main phases: (1) discovery/accusation, (2) examination, and (3) analysis. Each phase included a number of investigative processes (e.g., search and collection, recovery, harvesting) and profiling stages that consisted the four strategies of BEA (i.e., equivocal forensics analysis, victimology, crime scene characteristics, offender characteristics). The model also included specific details that described the input (e.g., offender skill level, MO) and output (e.g., evidence location, anti-forensics) within each stage.

To evaluate the model, the authors used a simulation of cyberstalking behaviour, which was analysed using DF techniques alongside BEA. A selected set of behaviours were simulated on two virtual machines that represented the offender and the victim. The behaviour used for the

test focused mainly on email communications, instant messaging conversations, social network activities, and some basic anti-forensic techniques. It also included other behaviour to make the simulation close to real life activities (e.g., web surfing, search queries). The results mainly focused on identifying the location of evidence on both the victim's and the offender's machines. It provided minimum detail about victim or offender behaviour, probably due to the fact that it was tested on a simulation that provided limited offender and victim activities. The evaluation, however, simply demonstrated the use of the outlined methodology. Testing the model on real cases is important as it would produce more detailed information on the offender, victim, and dynamics of the crime.

Silde and Angelopoulou (2014) recognised BEA mainly as an instrument of triage (i.e., a way to focus DF investigations on locations that are more likely to contain relevant evidence). They utilised behavioural profiling of the offender to assist in the DF investigation of cyberstalking crimes by providing insights into the possible locations of evidence, probable MO, and traces of anti-forensics. The authors focused on the technical phase of the methodology by using digital evidence (e.g., use of specific anti-forensic tools, communication files, registry files) to guide the search and recovery of evidence. They referred to the use of BEA stages in conducting the investigation, yet, they did not offer any guidelines on how to conduct these stages within the different phases of the process. The diagram of the proposed model represented the high-level process with the term *profiling stages* inserted between the investigation processes. They also touched on offender motivations, MO, and skills, yet without providing sufficient practical guidance on how to establish this information.

The evaluation methodology used in this study was not sufficient to assess the applicability and utility of the model. Since a simulation of a predefined set of cyberstalking activities were used, the researchers were already aware of what to look for during the examination and analysis of the victim and offender machines. As such, this is not fully sufficient to show how following the model, for example, can provide investigative directions. Also, the simulation did not include enough realistic information to illustrate offender characteristics (e.g., motivations), which is important when investigating real cases. Further tests, on actual cases and related digital evidence, are needed to better evaluate the applicability and utility of the model.

2.5.2 Roger's Behavioural Analysis Model

Rogers (2015) argued that the field of digital forensics seems to put more emphasis on computer science and engineering principles (e.g., file carving, hash functions), while paying less attention to traditional investigative approaches. As a result, the investigative process seems to be mainly concerned with data collection with less focus on examination and analysis of the data. He proposed a DFIPM that incorporated BA into the process of DF investigation. The

proposed model included six phases: (1) case classification, (2) context analysis, (3) data collection, (4) statistical analysis, (5) timeline analysis/visualisation, and (6) decision/opinion. He provided a brief description of each stage, with a specific focus on the *statistical analysis* and *timeline analysis/visualisation* phases.

Classification refers to identifying the category of case under investigation (e.g., fraud, cyberstalking, identity theft). *Context analysis* involves understanding the circumstances of the case to provide insights into the possible locations of relevant evidence. During the *collection* phase, the DF investigator works with the behavioural analyst to search for, and collect data relevant to the case, and sort them in preparation for analysis and interpretations. The *statistical analysis* phase focuses on conducting frequency analysis on the available data to assist in identifying and interpreting patterns that might be present. For example, frequency analysis can be performed on files that store data related to the user's online activities (e.g., cache files, web history files) to identify patterns related to preferred visited web pages, and types of uploaded/downloaded files. The outcome of this phase can then be used to create an online behavioural profile of the user. *Timeline analysis/visualisation* aims to combine results from the *statistical analysis* phase with their associated timestamps (e.g., timestamps of downloading specific files, visiting web pages) to visualise usage of the computer. This can further assist the investigation, for example, by associating the computer usage at a specific time with a specific individual (in cases where the computer has multiple users). The *decision/opinion* phase concerns producing the final report, which addresses the investigative questions presented at the start of the investigation. In this phase, the investigator utilises all the results from the previous phases to suggest the most likely reconstruction of the offence events, or the most likely characteristics of the offender (in cases of unknown offender).

Rogers (2015) employed three case studies to illustrate the use of the model in real cases. The first case involved the murder of an infant (8 months old), with two main suspects: the mother, and her boyfriend. The autopsy showed that the cause of death was trauma to the stomach. It also indicated that the infant had been physically abused over a period of time. Both the mother and the boyfriend denied being responsible for the murder, and provided mixed stories regarding their presence at home at the time of the infant's death. A single computer was shared (single user account) by the two suspects, which was seized along with their mobile phones for forensic examination. The DF investigator collected data including Internet history, web searches, social media, and cell tower data. Timeline analysis was performed on the data, and a behavioural analyst created a behaviour baseline for each of the two suspects. He also used work and class records for the mother to identify timeframes where the mother was not at home. Frequency analysis conducted on the most visited websites, and search terms performed by each of the two suspects, showed that the boyfriend had been searching the Internet for information

related to the type of injury sustained by the child. Finally, all the related evidence that was collected was correlated with a timeline in a visual diagram and presented to court, where the boyfriend admitted to the offence.

The other two cases involved arson murder, and possession of SEIC. Similar to the first case study, the arson murder case mainly employed frequency analysis and timeline analysis to create online behavioural profiles of the two suspects, and determine which of them was most likely to have committed the crime. The SEIC case involved a law enforcement officer who was arrested for downloading and possessing SEIC. The officer claimed that he had been investigating SEIC websites privately and had been reporting his findings to the authorities. A review of seven years of Internet history was conducted. Timeline analysis and frequency analysis were employed to determine the real motivation of the suspect. It was used to identify whether his activities were consistent with his claims, or with someone with a sexual interest in children. Frequency analysis showed that the most visited SEIC websites were related to underage teenage boys. Timeline analysis showed that during the seven years in question, only a few reports were made, which did not correspond to times when intense activity on SEIC websites were conducted. It was concluded that the suspect's activities were not consistent with his claims, and he was prosecuted.

Rogers (2015) demonstrated the application and usability of his model on different categories of crimes (e.g., arson, murder, SEIC). However, while the model constituted six phases, Rogers (2015) focused mainly on two of the phases: the benefits of conducting (1) frequency analysis and (2) timeline analysis/visualisation in DF investigations. Finally, the study did not offer a working framework with guiding steps that DF investigators can follow when investigating digital crimes.

Despite the limitations identified in the two previous models, they offered a useful insight into the development of the model proposed later in this research (Chapter 7).

2.6 Sexually Exploitative Imagery of Children (SEIC)

Commonly known as child pornography, the online sharing and distribution of Sexually Exploitative Imagery of Children (SEIC) is a form of offending which involves the production, distribution or possession of any visual depiction of children and young people (under a certain age) engaging in sexually explicit activity (Akdeniz, 2016, Clough, 2010, Houtepen et al., 2014). The online sharing and distribution of SEIC may also involve the digital transformation of non-sexual pictures of children into pornographic material, the use of computers to digitally design and generate virtual SEIC, or the online live streaming of sexual abuse of children (Hewitt and Marcum, 2016, Krone, 2004).

This section will focus on three overlapping areas of research in SEIC offending: offender characteristics, typologies and theories of motivation, and victim characteristics. These themes have been selected as they are related to conducting behavioural analysis and will be referred to in a later chapter in discussion of a study conducted within this research (Chapter 4).

2.6.1 Prevalence of Online SEIC

Although the production and possession of SEIC is not a new phenomenon, advances in technology and the widespread adoption of the Internet have created more opportunities for individuals with deviant sexual tendencies to access and disseminate SEIC (Akdeniz, 2016, Hewitt and Marcum, 2016). The capacity to instantly access information, exchange files, and the relative absence of effective legal regulation and geographical boundaries online have also encouraged this type of offending (Beech et al., 2008, Hewitt and Marcum, 2016, Wortley and Smallbone, 2006). This has facilitated the proliferation of commercial activities related to SEIC, and has been a major contributor to increases in the amount and quality of SEIC circulating online (Henshaw et al., 2015, Wortley and Smallbone, 2006). As such, individuals with deviant sexual tendencies have used the Internet as a medium to easily access, disseminate, and circulate SEIC.

Studies conducted in different parts of the world indicate that the online possession and dissemination of SEIC is highly prevalent. For example, a study conducted in the United States (US) for a period of a year focusing on a Peer-to-Peer (P2P) filesharing program, Gnutella, found that around 250,000 computers in the US were being used to share and receive SEIC (Carnes, 2013). The Internet has largely been credited for this increase with many of the victims being those who are unable to protect themselves (Carnes, 2013). In the United Kingdom (UK), research conducted by BBC News collected data from 34 police forces in England and Wales, and found a 48% increase in the number of online SEIC crimes between 2007 and 2011 (Cafe, 2013). The Internet Watch Foundation annual report (2016) revealed that offenders are increasingly using new techniques to host SEIC, and disguise it from authorities. Websites using Generic Top Level Domains (gTLDs) to disseminate SEIC increased by 258% compared to 2015. Websites' use of obfuscating techniques to hide SEIC material from authorities, and leave hints to offenders on how to reach the material, has also increased by 112% compared to 2015. It also revealed that worldwide domains used to host SEIC have increased by 21% than 2015. Statistics from the Dubai Police in the UAE indicate that during the years 2010-2014, the Department of Electronic Evidence has witnessed a 23% increase in cases involving online possession and dissemination of SEIC (2014).

2.6.2 Characteristics of SEIC Victims

There is very limited research evidence currently available that describes demographics and characteristics of SEIC victims. The Internet Watch Foundation (2016) reported that their work had confirmed 57,335 URLs containing SEIC imagery in 2015. Analysing the content of this material showed that the majority of victims were females (89%). It also showed that 53% of the children appeared to be aged as 10 or under, revealing a steady decrease in SEIC depicting younger children from 2015 (69%) and 2014 (80%). There was, however, an increase in SEIC images depicting children assessed as being aged 11 to 15 years (45% in 2016 compared to 30% and 18% in 2015 and 2014 respectively). A possible explanation for this increase is the new trend of "self-produced" content among youngsters; where they use webcams to capture sexual images of themselves and share them online (Internet Watch Foundation, 2016). The literature also suggests that in terms of the relationship between victims and producers of SEIC, the offenders are usually known to the victims prior to the production of the SEIC imagery (e.g., family member, teacher, guardian, someone whom the victim met online) (Bryce, 2017).

2.6.3 Characteristics of SEIC Offenders

There is a small but developing body of empirical research examining the behaviour, demographic and psychological characteristics of online SEIC offenders. As online SEIC offenders started entering the criminal justice and treatment systems, greater understanding of their psychological characteristics and motivations is required (Wolak et al., 2008). Opportunities to understand this group of offenders arise when they are arrested and charged. Studies conducted by law enforcement agencies on offenders convicted of child-related sexual offences, both online and offline, indicate that a large proportion of offenders are well known to the children involved, and/or wield significant authority over them (e.g., teachers, members of the clergy, close family members) (Babchishin et al., 2015, Shelton et al., 2016, Wolak et al., 2008).

A study conducted in the US, for a period of 12 months, collected data from a sample of law enforcement agencies about the characteristics of 2,577 online SEIC offenders. The results indicated that the majority of the offenders were of Caucasian ethnicity (92%) and over 25 years of age (86%). It also found that 11% of the offenders were known to have a history of violence, and 10% had a history of offences against minors (Wolak et al., 2003). A UK study of 90 online SEIC offenders showed similar results, with 82% of offenders being of Caucasian ethnicity. 7% of the sample also had convictions for previous sexual offences, 17% for non-sexual offences, and 3% for violent offences (Webb et al., 2007).

Newer studies found similar results in relation to offender demographics. A study of 251 resolved FBI SEIC cases (Shelton et al., 2016), where offenders were convicted, showed that offenders were exclusively males. 97% were Caucasian, while the other 3% constituted Asian, African-American, Hispanic, and Native American ethnicities. 191 cases recorded the offender's marital status. Of these, 43% were never married, 34% were married, 12% were divorced, 5% were separated, and 2% were widowed. Also, from 107 of the offenders, 72% obtained education beyond high school, with the highest being a graduate degree (11%). From the known employment history of 215 offenders, only 3% were unemployed. Offenders were employed in a variety of work sectors including business (21%), computer-related (19%), constructions (17%), positions of trust (19%) (e.g., education, mental health, medical, public safety), sales (10%), military (7%), transportation (5%), and students (3%). Finally, the criminal history of 250 of the offenders indicated that 28% (n=71) had prior arrests. Of these, 27% were arrests for felony sexual crimes against children, and 10% were arrests related to the possession and dissemination of SEIC.

Overall, studies suggest that apart from the majority being of Caucasian ethnicity, online SEIC offenders are a heterogeneous group from diverse backgrounds, levels of society, levels of education and age groups, with few having a history of sexual or non-sexual offences (Burke et al., 2002, Galbreath et al., 2002, Seigfried-Spellar, 2014, Seto and Eke, 2005, Wolak et al., 2011). Also, compared to offenders who commit physical sex offences against minors, evidence show that online SEIC offenders were generally better educated, mostly employed, were in a relationship, and were less likely to have a criminal history (Babchishin et al., 2015, Magaletta et al., 2014, Shelton et al., 2016).

2.6.4 Offender Typologies and Theories of Motivation

There are a variety of motivating factors for an offender's collection or possession of SEIC, ranging from those which are focused on a sexual interest in children to those which relate to non-sexual pathological Internet use (Beech et al., 2008, Magaletta et al., 2014, Merdian et al., 2013). Previous studies suggested that motivations vary among offenders, and that they generally have more than one motivation for their behaviour (Beech et al., 2008, Magaletta et al., 2014, Merdian et al., 2013). To better understand motivations for SEIC offending, it is important to consider relevant theories and developed typologies. This section examines (1) sexual and non-sexual motivations for SEIC offending, and (2) typologies of SEIC offenders.

2.6.4.1 Sexual and Non-Sexual Motivations

The two main sexual motivations for SEIC offenders are sexual interest in children and the equivalent sexual gratification provided by engagement with the material (Elliott and Beech,

2009, Seto et al., 2006). Non-sexual motivations for SEIC offending consist of initial curiosity, collecting behaviour, attempting to avoid real-life problems and its accompanying stress and dissatisfaction, and to be able to have a better social life online by communicating with like-minded offenders (Quayle, Vaughn, & Taylor, 2006).

Quayle and Taylor (2002) identified: (1) sexual arousal, (2) pleasure in collecting behaviour, (3) avoiding real-life problems, (4) social relationships, (5) therapy, and (6) manifestation of Internet addictive properties. Their findings were based on semi-structured interviews with thirteen male offenders convicted of the online downloading and possession of SEIC files. The interviews mainly constituted open-ended questions to elicit narratives from the interviewed offenders. They were transcribed, coded, and analysed for patterns of motivating factors. The authors also used quotations from the interviews to illustrate the analysis. The sample used was relatively small and does not represent the diverse population of SEIC offenders. However, the study provided rich descriptions of the identified motivational factors.

In terms of addiction to the Internet, Cooper and Griffin-Shelley (2002) identified three factors that attracts SEIC offenders to the Internet as a medium to collect SEIC: (1) accessibility, (2) affordability, and 3) anonymity.

With regards to the sexual gratification, therapeutic, and reality avoidance aspects of motivation, Henry et al. (2010), identified three groups of SEIC offenders: (1) normal population profile, (2) emotionally inadequate profile, and (3) sexually deviant profile. Their typology was based on the analysis of the data of 633 male SEIC offenders who completed a survey package containing different scales. It was obtained from the UK National Offender Management Service (NOMS). 93.8% of the sample were producers, 6% were possessors, and 0.2% had enticed a child into sexual activity. The data was derived from standard screening instruments used by the UK Probation Service as part of their routine assessment package. The sample used in this study mainly consisted of producers of SEIC, which limits generalisation to other groups of SEIC offenders (e.g., viewers, traders).

Another theory of SEIC motivation was offered by Beech, Elliott, Birgden, and Findlater (2008), who identified four motivational factors for SEIC offending: (1) to nurture their existing or developing sexual interests in children, (2) to use the collected imagery as part of a contact offending, (3) impulsivity and curiosity, and (4) financial gain. Their motivational theory was concluded after reviewing existing typologies on SEIC offenders such as those developed by Lanning (2001), Alexy et al. (2005), and Krone (2004). Their theory was not empirically verified, and the authors emphasised the need for further research to verify the identified SEIC offender motivational factors.

2.6.4.2 Typologies of SEIC Offenders

Researchers have attempted to categorise SEIC offenders based on their behavioural and psychological characteristics. These factors include offender motivations for possessing SEIC, level of technical skills, level of involvement in dissemination or possession of SEIC, participation in online SEIC communities, use of countermeasures to avoid detection, and progression to physical sexual abuse (Alexy et al., 2005, Krone, 2004, Webb et al., 2007). Based on these factors, Krone (2004) developed a typology to describe SEIC offenders that included nine categories:

1. The **browser** refers to an individual who initially views SEIC accidently (e.g., through pop-ups, entering an unsuspecting web page). The individual may or may not have intentionally saved SEIC on their computer. This can be determined by an examination of the surrounding facts and digital evidence. The browser does not employ any security measures to evade detection, and does not communicate with other offenders online.

2. The **private fantasy offender** creates SEIC representing their sexual fantasy, has the material for their private use, and do not share it with others. They do not communicate with other offenders online, nor do they employ any security measures to hide their SEIC material.

3. The **trawler** is an offender who searches for SEIC online as part of wider deviant sexual interests. These offenders employ no or few security measures to mask their behaviour and do not network with other offenders. This group includes the omnivorous user, the sexually curious user and the libertarian. The omnivorous user is generally inclined towards a wide range of sexually explicit material with SEIC being part of their deviant interests, but not the main focus. Krone (2004) describes the sexually curious user as one who has not pursued SEIC although they may have experimented with it. This description does not provide a clear understanding as to how the trawler had "experimented" with SEIC, however, Krone (2004) does not provide any further clarification of this category. A libertarian holds the view that they are free to access or possess any material they are interested in (Wolak et al., 2008).

4. The **non-secure collector** uses websites and chat rooms that do not employ security restrictions (e.g., passwords, encryption) to buy, trade, or download SEIC. They have a higher degree of communications with other online SEIC offenders than trawlers.

5. The **secure collector** obtains SEIC from secure communities and online groups. They usually exhibit strong desires to create large collections of SEIC.

6. The **online groomer** seeks online contact with minors with the intention of forming a relationship which progresses to online or physical sexual contact. They use SEIC to reduce the child's resistance to engaging in sexual activities.

7. The **physical abuser** engages in physical sexual abuse of minors and uses online SEIC to complement or facilitate offending. They make records of their behaviour for their own personal use without intending to distribute or share them online.

8. **Producers** are offenders who commit physical sexual abuse of minors, and record their conduct, creating SEIC files to share with others.

9. **Distributors** may not necessarily have any sexual interest in children, but are mainly interested in monetary gain from disseminating SEIC.

Krone (2004) stated that the proposed typology was the result of combined work by the Australian Institute of Criminology and the Australian High Tech Crime Centre. No further details were provided about the type of data and analysis that formed the basis of the development of this typology. The typology, however, appears to be the most comprehensive to date, and was developed to aid in criminal investigations rather than in clinical treatment of offenders. Therefore, this typology was identified as the most appropriate to refer to in the later chapters of the thesis; mainly in discussions related to the digital forensics investigations of SEIC cases (Chapter 4).

The behaviours associated with each of Krone's different categories of offending generate specific forms of digital evidence which can be recovered from computers and other devices during DF investigations. For example, a *browser's* computer would have evidence of SEIC files stored on Internet history and cache folders, while a *groomer's* computer could reveal chat logs containing conversations with potential victims. This can be examined using BA in order to build a specific profile of an offender which can then be used to determine the nature of their offending behaviour, association with others with similar interests and risk of progression to physical sexual abuse. This information can then assist in criminal investigations and prosecution.

Elliott et al. (2009) identified four types of SEIC offenders based on their motivation to offend: (1) periodically prurient offenders, (2) fantasy only offenders, (3) direct victimisation offenders; and (4) commercial exploitation offender. The first group includes offenders who access SEIC impulsively or out of curiosity. Their behaviour is not specifically related to sexual interest in

children as they view SEIC occasionally as part of a general interest in pornography (e.g., extreme pornography). The second group consists of offenders who do not have any known history of contact sexual offending, though they possess and trade SEIC to nurture a sexual interest in children (e.g., Osborn & Beech, 2006; Webb, Craisatti, & Keen, 2007). The third group includes offenders who use the Internet as a means to facilitate contact and non-contact sexual offending, including SEIC and the online grooming of children for the commission of offline sexual offences (Krone, 2004). The final group are offenders who produce or trade images for financial gain (Lanning, 2001). This categorisation was derived from earlier behavioural typologies identified by Lanning (2001), Sullivan and Beech (2003) and Krone (2004), integrating them into the previously mentioned groups.

Merdian et al. (2013) proposed a model for classifying SEIC offenders derived from existing theories and typologies of SEIC offenders. Their identified subgroups were based on three dimensions: (1) type of offending, (2) the motivation behind offending, and (3) the situational and social engagement in the offending behaviour. As for the first dimension offenders were classified into two main groups: (1) fantasy-driven, and (2) contact-driven. Further motivational subgroups were identified for the fantasy–driven group: (1) pure financial gain, (2) generally deviant, (3) paedophile, and (4) other (non-sexual). With regards to social engagement in the offending behaviour, the fantasy-driven group had subgroups of engaging in either low or high levels of networking, with higher involvement indicating greater severity of the offence. The typology was designed mainly to assist in the selection of appropriate assessment and treatment measure for SEIC offenders. The authors also emphasised the need to test and verify the applicability of the model even though it was developed on the basis of earlier studies (Merdian et al., 2013).

2.6.5 Applying the Theories to Digital Forensics and SEIC

Any model of DF evidence collection and investigation relating to online SEIC offenders should consider the implications of existing theories about the motivations and characteristics of SEIC offenders and their behaviour. A consideration of the sexual and non-sexual motivations of SEIC offenders, for example, can guide the DF investigator to consider evidence that indicates both sexual and non-sexual motivations (e.g., chat logs reflecting conversations to lure potential victims into sexual activity, emails revealing the trade of SEIC). The typologies developed by researchers are helpful in attempting to create a profile of the offender that can then guide the DF investigation. Once an offender, for example, is identified as a *distributor*, the presence of evidence of SEIC on the offender's digital devices should encompass that of a *distributor*, and not a mere *browser*. A browser, for instance, may not have connections with other SEIC offenders compared to a *distributor*. In this regard, the fact that an offender is likely

a *distributor* requires a different investigation in terms of scope and depth than when they are a *browser*.

It is important, however, for the DF investigator to consider other possibilities when investigating a SEIC case, and not to be guided solely by the initial classification of an offender. For example, a digital device of an initially identified *browser* can reveal evidence that aligns with a *distributor*. A consideration and interpretation of the different available evidence helps to construct a clearer picture of the crime events, as well as establishing the motivation and intention of the offender, all of which aids in prosecution.

2.7 Cyberstalking

Despite a lack of a universally accepted definition of cyberstalking, the term generally refers to the use of the Internet, email and other forms of telecommunication technologies to pursue or harass another person (Nobles et al., 2014, Strawhun et al., 2013, Vasiu and Vasiu, 2016). Cyberstalking is not just the mere annoyance of unsolicited email but it is deliberate, methodical and persistent, and it may involve a known or unknown person (Harvey, 2003). This communication does not end when the victim asks the cyberstalker to cease contact and it often contains disturbing and inappropriate material (Bocij, 2004, Strawhun et al., 2013). Bocij and McFarlane (2002) comprehensively define cyberstalking as a collection of behaviours where a person, groups of persons or even organisations use information technology with the intention of harassing another person or a group of people. These behaviours include, but is not limited to, conveying threats and false accusations, defamation, data theft, identity theft, computer monitoring, and extortion. The literature shows a significant overlap between the definitions of cyberstalking, cyber-harassment, and cyber-bullying (Vasiu and Vasiu, 2016). However, this research will refer to the previously defined behaviours as cyberstalking.

While in the traditional form of stalking an individual is persistently watched, followed or harassed with unsolicited and obsessive attention, another dimension is added when computers are used as they increase the potential reach of the obsessed stalker (Henry and Powell, 2016, Navarro et al., 2016). When emails are utilised by the stalker, the victim may be bombarded with material wherever they are; while the stalker remains unknown instilling constant fear in the victim or making them feel threatened (Harvey, 2003). The use of technology also allows offenders to hide their identity. Being anonymous makes it easy for the offender to target the victim without the need or ability to see their physical or psychological response (Ashcroft, 2001, Henry and Powell, 2016). Technological devices also have a distancing effect which can encourage offenders to act and express themselves in ways that they would not in a traditional face-to-face encounter (Kowalski et al., 2012). Offenders can also use multiple "aliases"

allowing multiple online personas to be built, complicating the investigation of cyberstalking cases (Stephenson and Walter, 2011).

With the advent of the Internet, online forums have provided breeding grounds where people can verbally assault each other as they spend hours chatting with each other and gossiping. Social networking sites such as Facebook, Twitter, MySpace, and Instagram among others allow users to create individual profiles and interact with others online (Navarro et al., 2016, Strawhun et al., 2013). The publication of personal information online increases the vulnerability of a person to being cyberstalked (Boon and Sheridan, 2002). The intention of a cyberstalker is usually to harm the targeted victim while hiding their behaviour and identity behind the untraceable distance of technology (Vasiu and Vasiu, 2016).

This section will focus on four overlapping areas of research in cyberstalking offending: forms of cyberstalking, offender characteristics and typologies, theories of motivations, and victim characteristics. These areas have been selected as they are related to conducting BA and will be referred to in a later chapter presenting a study conducted as part of the programme of research (Chapter 5).

2.7.1 Forms of Cyberstalking

Studies conducted before the rise of smartphones identified three main ways in which cyberstalking is performed: (1) email stalking, (2) Internet stalking, and (3) computer stalking. In the physical world, the most common form of stalking may involve sending mail, telephoning and actual physical surveillance (Burgess and Baker, 2002). However, sending unsolicited emails is a common form of harassment employed by cyberstalkers; usually containing obscene or threatening material (Cavezza and McEwan, 2014, Ogilvie, 2000). Email stalking may also involve the cyberstalker harassing the victim by sending them viruses or high volumes of electronic junk mail or spam mail (Cavezza and McEwan, 2014, Henry and Powell, 2016).

While sending viruses or telemarketing solicitations may not amount to cyberstalking, the sending of repeated communications of this nature with the intention of intimidating the recipient constitutes cyberstalking (Cavezza and McEwan, 2014). Email stalking is a close replication of the patterns of traditional stalking which normally employs telephoning and sending mail. The email as a medium integrates the immediacy associated with a telephone call and the degree of separation associated with letters (Ogilvie, 2000). Just like telephone stalking, email stalking involves uncalled for and threatening incursion into the private space of the victim.

Cyberstalkers can also employ the global communication opportunities offered by the Internet to comprehensively slander and endanger the targeted victim (Navarro et al., 2016). As opposed to the private nature of email stalking, Internet stalking allows the behaviour to take on a more public dimension (Navarro et al., 2016). Internet stalking involves a wide range of stalking behaviours such as monitoring the victim online, posting false information about them on social networking sites, and using VoIP technology to spoof their outgoing phone number (Eterovic-Soric et al., 2017).

In the third form of cyberstalking; computer stalking, the offender exploits the workings of the operating system and the Internet connection of the victim's computer with the intention of taking control of it. Many people are not aware that a Windows based computer connected to the Internet can easily be identified by another person using their Internet connection (Burgess and Baker, 2002). This computer-to-computer connection enables the intruder to exercise control over the victim's machine. This vastly reduces the buffer between the cyberstalker and the victim, making it easy for the offender to directly communicate with the victim whenever their computer connects to the Internet. Once the victim's computer connects to the Internet, the cyberstalker takes control of it forcing the victim to disconnect from the Internet or relinquish his or her Internet protocol address (Ogilvie, 2000). Computer stalking may include real time recording of every keystroke (real-time key logging) and viewing of the desktop of the victim in real time.

As smartphones have evolved to integrate applications for private communication services (e.g., emails, online messaging), social media (e.g., Facebook, Twitter), and trackers (e.g., Phone Tracker, Find My iPhone), offenders have demonstrated a notable shift towards using these tools in their stalking offences (Eterovic-Soric et al., 2017). A study conducted by Woodlock (2017) identified smartphones, social media, emails, and GPS (Global Positioning System), as the most commonly used technologies to facilitate stalking of women in the context of domestic violence. A UK study that surveyed 274 victims of cyberstalking and online harassment found that emails, SMS messages, and mobile calls were most commonly used in their victimisation (Al-Khateeb et al., 2017).

2.7.2 Prevalence of Cyberstalking

There is evidence that cyberstalking is prevalent in the world today. A Canadian study (Hango, 2016) found that 17% of 15-29 year old have experienced forms of cyberstalking and cyberbullying between 2009 and 2014. The European Union Agency for Fundamental Rights (2014) published a report based on interviews with 42,000 women across the European Union (EU). 11% reported experiencing sexual online abuse through social media, email, or SMS. A study interviewing 109 female political online bloggers in Germany, Switzerland, the UK, and

the US found that 73.4% have experienced negative online incidents including abusive comments, stalking, rape threats, and death threats (Eckert, 2017).

2.7.3 Characteristics of Cyberstalking Victims

An Australian study (Woodlock, 2017) that surveyed 46 cyberstalking female victims found that 92% were Anglo-Australian, 91% heterosexual, 9% bisexual, 9% as having disability, and 17% as a parent. Their average age was 35 years. A UK study that surveyed 274 victims of cyberstalking found that 74% were females, and 21.3% males (Al-Khateeb et al., 2017). Their average age was 36.5 years, and they were regular users of the Internet (75% checking their emails over 5 times daily). The study also found that the offence was most commonly committed through personal communication channels (e.g., personal emails, SMS messages), rather than public venues (e.g., blogs, forums). This suggests prior knowledge of the offender rather than harassment by a stranger. This is consistent with the results of another study examining the relationship between victims and offenders in a sample of 1,040 college students which found that ex-intimates were most likely to be involved in cyberstalking offences, while strangers were most commonly involved in offline stalking (Heinrich, 2015).

A UK study (Worsley et al., 2017) that surveyed 100 victims of cyberstalking found that 65% were females, and the average age was 38.9 years. In 50% of the cases, the victim had little to no prior relationship with the offender (25.5% acquaintance, 24.4% strangers). Other identified relationships included casual dating (13.8%), ex-intimates (11.7%), work colleagues (6.3%), close friends (4.2%), ex-partners (2.1%), pupil (1%), and relative (1%).

Short et al. (2015) employed a survey to gather data on the victimisation experiences of 353 self-defined victims of cyberstalking. Demographics showed that the majority of victims were females (68%), though a high prevalence of male victimisation was also identified (32%). The average age of victims was 38 years. In terms of the victim-offender relationship, the most commonly reported categories were ex-intimates (27.9%), strangers (21.7%), and work colleagues (6.3%).

Considering risk factors across studies, findings largely show that females are more likely to be victims of cyberstalking, with an increasing proportion of male victims as well. The most common victim-offender relationships were ex-intimates, followed by strangers and work colleagues. Individuals who engage in online activities more often were more likely to be at risk of victimisation.

2.7.4 Impacts of Cyberstalking on Victims

Researchers and scholars have emphasised the amount of harm that cyberstalking can cause its victims (Vasiu and Vasiu, 2016). Studies have identified a number of negative psychological effects commonly experienced by victims. For example, surveying 100 victims of cyberstalking, Worsley et al. (2017) found that fear, anxiety, and depression to be the predominant emotional impacts of cyberstalking. An exploratory study that thematically analysed email interviews with 12 victims of cyberstalking identified the experience of stress, feeling hurt, paranoia, insomnia, anger, fear and depression (Jansen van Rensburg, 2017). Analysing data collected from their victim sample (n=353), Short et al. (2015) found that 32.7% had symptoms of Post-Traumatic Stress Disorder (PTSD). The sample also showed levels of anxiety and distress higher than that identified in the general population.

2.7.5 Cyberstalking Typologies and Motivation Theories

2.7.5.1 Background on Typologies of offline Stalking

Earlier studies sought to understand offline/traditional stalkers, through developing typologies based on their behaviour and motivations. Based on 74 cases investigated by the Threat Department of the Los Angeles Police Department, Zona et al. (1993) developed a typology of stalkers using the Diagnostic and Statistical Manual of Mental Disorders. According to their analysis, they identified three types of stalkers: (1) love obsessionals, (2) erotomanics, and (3) simple obsessionals. Love obsessionals were stalkers who had a fanatical love for their victims, although there is no relationship between them (e.g., being obsessed with celebrities). Erotomanic stalkers are deluded by the belief that the victim is in love with them. Both love obsessionals and erotomanics often suffer from bipolar disorder or schizophrenia, or other mental illnesses. Simple obsessionals are stalkers that were once involved romantically with their victims, and wish to reconnect with the victims or seek revenge by harassing them (Zona et al., 1993).

Another typology was advanced by Harmon et al. (1995) after a review of case files of offenders referred to the Criminal and Supreme Courts of New York's Forensic Psychiatric Clinic. They defined stalkers based on the attachment between the stalker and the victim, as well as their prior relationship. Based on the nature of attachment between the stalker and the victim, the offenders were classified as angry, amorous, affectionate or persecutory. Stalkers who had prior relationships with their victims were classified as personal, employment, professional, acquaintance and media. They noted that affectionate or amorous stalkers most often suffered from features of erotomania, while stalkers of ex-intimates possessed personalities characterised by paranoia and narcissistic tendencies.

After examining 25 individuals charged with the offence of stalking, Kienlen et al. (1997) classified stalkers into two groups: (1) psychotic, and (2) non-psychotic. Psychotic stalkers possess symptoms that ranged from schizophrenia, bipolar disorder and delusions. Non-psychotic stalkers suffer from disorders such as personality disorders, alcohol and drug abuse and mood disorders.

While the offline stalker typologies have also been applied to cyberstalkers, McFarlane and Bocij (2003) criticised these typologies as not being fully sufficient to describe cyberstalkers. The, they encouraged the creation of typologies that are designed specifically for cyberstalkers and reflect the specific dynamics of this form of offending.

2.7.5.2 Cyberstalking Typologies

Cyberstalking has garnered great interest in interdisciplinary research (Lowry et al., 2013). A number of efforts have been made to propose typologies for the behaviour and motivations of cyberstalkers. These are helpful because they focus on dimensions of cyberstalking that allow a researcher to explain how and why cyberstalking occurs. The typologies, therefore, focus on the behaviour and motivations of cyberstalkers and include the following: (1) McFarlane and Bocij's Typology, (2) the Keppel/Walter Sub-Types, (3) Bojic's Technological and Social Motivation Typology, and (4) Lowry et al.'s Behaviour and Motivation Taxonomy.

2.7.5.2.1 McFarlane and Bocij's Typology

McFarlane and Bocij (2003) offered one of the first typologies that emerged from exhaustive studies of earlier typologies on offline stalkers, and of data on victims of cyberstalking. They developed a typology based on interviews with 24 cyberstalking victims which identified four categories of offenders:

1. **Vindictive cyberstalkers** are characterised by relentless harassment of their victim without a specific reason. They are more malicious and ferocious, threatening and harassing than the other types. They will escalate to offline stalking and the majority of them have a criminal record. They have a medium to high level of computer literacy and would use a variety of methods to cyberstalk their victims (e.g., identity theft, excessive spamming, mailbombing). They use viruses and Trojan horses to compromise their victims' computers and gain control over them. They frequently send messages to victims with disturbing content, which indicate the possible presence of mental illness.
2. **Composed cyberstalkers** target their victims in a calm and poised manner aiming to cause them constant annoyance and irritation. They have no desire to establish a relationship with their victims, and are motivated to cause them distress. They have a

medium to high level of computer literacy. They usually have no prior criminal record and no prior history of victimisation.

3. **Intimate cyberstalkers** are characterised by the desire to attract the attention or affection of their victims. Their primary purpose is to establish a relationship with the victims due to infatuation and obsession. They usually have detailed knowledge of the person being targeted, and utilise tools such as emails, discussion groups, and electronic dating sites to pursue their victims. Their computer literacy ranges from fairly low to high. Unlike other types of cyberstalkers, they are more diverse and may have had previous relationships with their victims.
4. **Collective cyberstalkers** consist of a group of individuals harassing their victims through the use of communication technology. They have a higher level of computer literacy than the other types. This category of offenders is motivated by seeking revenge for actual or perceived injustices.

2.7.5.2.2 The Keppel/Walter Sub-Types

The Keppel and Walter (1999) typology, which focused on sexually oriented murderers, has been extended by Stephenson and Walter (2011) for assessing cybercrimes and profiling cyberstalkers. The four Keppel/Walter sub-types include: (1) power assertive, (2) power reassurance, (3) anger retaliatory, and (4) anger excitation. With regards to cyberstalking, Stephenson and Walter (2011) deemed power assertive and power reassurance as most applicable, and view anger retaliatory and anger excitation as rare in cyberspace.

1. The **power assertive** (PA) cyberstalker is motivated to have power and control over the victim. This type of offender is usually organised and has a high level of computer literacy. They utilise a variation of computer skills during the process of harassing their victim (e.g., anonymisation, remote access of the victim's computer). They would boast about their cyberstalking achievements anonymously on social networking sites, forums, and discussion groups. Their written communication to their victim would usually reflect their psychological need to maintain power, control, and authority. This would usually manifest in offline stalking leading to sexual related crime (e.g., rape, rape-murder).
2. The **power reassurance** (PR) type tends to be less organised than the PA. They usually feel insecure and need to reassure their self-confidence. They play out a personal fantasy through their cyberstalking and seek to engage their victims in their role play. They are less aggressive than PA stalkers, yet, they may escalate to offline stalking if the online stalking ceased to satisfy their fantasy. In terms of computer literacy, they are less skilled than PA cyberstalkers and would usually leave cyber trails (Stephenson and Walter, 2011).

3. The **anger retaliatory** (AR) type is driven by rage and hostility. They will express their inner anger towards a random target, or a victim that represents a symbol of the true cause of real or imagined wrongs. AR cyberstalkers do not usually escalate to offline stalking, and they are rarer than PA or PR cyberstalkers (Stephenson and Walter, 2011).
4. The **anger excitation** (AE) type is sadistic and seeks to achieve sexual gratification from the victim's suffering. Their activities are focused around terrorising the target by inflicting physical and psychological pain at increasing levels of aggression until the stalker achieves destruction of the victim. Like AR, this type of cyberstalker is rare because the ultimate destruction aim is less likely to be achieved in the online environment (Stephenson and Walter, 2011).

2.7.5.2.3 Bojic's Technological and Social Motivation Typology

Bocij (2004) had also proposed two categories for cyberstalking motivations: technological and social. According to Bocij (2004), "technology provides both the mechanism through which the individual can act and the protection needed against arrest or other punishment". He then lists technological opportunities for criminal offending that the Internet provides, including (1) easy access to computers and the Internet, (2) greater familiarity with technology, (3) a greater level of anonymity, (4) easy to disguise criminal activities, and (5) easy destruction of evidence (Bocij, 2004, McFarlane and Bocij, 2003). Additionally, Bocij (2004) states that the Internet creates social motivations for people to engage in misconduct. Social motivations include (1) a decontextualised medium unconstrained by social reality (Williams, 2006), (2) anonymity which creates disinhibition, and (3) dehumanisation of others driven by anonymity (Bocij, 2004).

2.7.5.2.4 Lowry et al.'s Behaviour and Motivation Taxonomy

To arrive at a working definition for cyberstalking, Lowry et al. (2013) focused on two dimensions of cyberstalking: behaviour and motivation. After a review of the existing literature on cyberstalking, the authors proposed three types of cyberstalking behavioural patterns: (1) secret cyberstalking, (2) indirect cyberstalking, and (3) direct cyberstalking. Recognising that a cyberstalker may have more than one motivation, Lowry et al. (2013) proposed a simplified and reclassified typology of cyberstalking motivations: (1) to fulfil the cyberstalkers' psychological needs regarding another person, (2) to instil fear in or gain control over a victim, (3) to seek revenge or punish the victim, and (4) to build a relationship with the victim.

2.7.6 Limitations of Cyberstalking Typologies and Motivation Theories

The studies mentioned above used inductive approaches in which the researchers used initial statistical data on specific offender behaviour to construct general conclusions and create broad

offender typologies. McFarlane and Bocij (2003) offer generalised description of cyberstalking offenders, which does not provide the level of differentiation required to be useful in digital forensics investigations (Stephenson and Walter, 2011). Similarly, the Keppel/Walter Sub-Types focuses on two broad sub-types (PR and AR), creating a generalised set of characteristics for the typical offender for each sub-type. Also, both typologies as well as motivation theories do not consider the digital evidence associated with the identified cyberstalker categories and motivations, nor do they provide a working framework for how these typologies can assist in the DF investigation of cyberstalking cases.

2.7.7 Applying the Theories to Digital Forensics and Cyberstalking

The broad nature of the developed theories and typologies of cyberstalkers limits their benefit in the DF investigation of these cases. These typologies were also mainly developed for clinical assessment and treatment of offenders, and not with investigation in mind. DF investigators, however, can use these typologies to broaden their understanding of the different motivations and intentions of offenders. As such, these typologies can be used to inform the context of the DF investigation of cyberstalking cases. Then, combined with case-specific data, the DF investigator can use this information to develop the reconstruction of the crime events (Rogers, 2015).

To provide greater utility in DF investigations, cyberstalking typologies must be further researched, updated, to provide more specific descriptions of offenders. The different types of digital evidence found in cyberstalking cases can be mapped onto the identified categories of offenders to be of more investigative utility to DF investigators.

2.8 Summary

Prior studies have contributed to the field of criminology in DF investigations by utilising inductive approaches to understand offender behaviour and motivation with cybercriminal domains (e.g., cyberstalking, SEIC). As such, most of the efforts made in this field depended on statistics and generalisation in painting a portrait of the typical offender in specific types of digital crimes. This generalised approach, however, is of limited use and does not make practical sense given the uniqueness and specificity of digital crimes (Rogers, 2003).

The utility of BA has gained attention in the field of DF in recent years. It has been recognised that, along with technical examination of digital evidence, it is important to learn about the individuals behind an offence, the victim(s) and the dynamics of a crime. This can assist the investigator in producing a more accurate and complete reconstruction of the crime, in interpreting associated digital evidence, and with the description of investigative findings.

Despite these potential benefits, the literature demonstrates a very limited body of knowledge of digital crime investigation that incorporates behavioural and motivational analysis in the process. There is even less that concerns the usability of BA in the examination and interpretation of digital evidence in these crimes.

Chapters 4 and 5 aim to fill this identified gap by testing the utility and applicability of BA empirically. Strategies of BA will be incorporated within the post-mortem digital forensics process in investigating real SEIC and cyberstalking cases in order examine its potential to develop greater understanding of the dynamics of specific crimes and improve their investigation.

The next chapter will describe the methodological approaches for data collection and analysis which will be used for this research.

3 METHODS

3.1 Introduction

This chapter presents a discussion of the research methodologies and paradigms which form the basis of the programme of research. It outlines the general methodology and procedures used throughout the studies included within the thesis. First, the chapter introduces four research principle models: the positivist, interpretive, critical, and pragmatic paradigms. Then it briefly covers research methodologies and strategies. After that, the chapter discusses the selected model for this research, and provides a detailed explanation and justification for the chosen methods and strategies (i.e., research philosophy, research methods, and research strategies). Finally, it describes the study design, data analysis, and limitations of each conducted study.

3.2 Review on the Research Aims

A research methodology denotes a systematic plan to collect, interpret and analyse a set of data in order to answer specific questions and gain new knowledge on a specific topic (Kothari, 2004). It considers the theories, concepts, and logic behind the various steps and techniques selected by the researcher (O'Leary, 2013). An effective research methodology facilitates the smooth performance of the various research operations, increasing the efficiency of the research and yielding maximal information with the use of minimal resources (Kothari, 2004). Selecting an appropriate methodology depends on a number of factors that include research questions, ethics, as well as time and money constraints (Kothari, 2004). Flick (2015) specifies that research characteristics such as aims and types of data to be collected are crucial factors in determining research methodology.

This research sought to build on previous work by scientific researchers and practitioners in developing a Digital Forensics Investigation Process Model (DFIPM). Its main aim was to

employ a multidisciplinary approach to develop a model that incorporates strategies of Behavioural Analysis (BA). It focused on a specific investigative phase: the post-mortem in-lab examination, analysis, and interpretation of digital devices associated with computer-facilitated interpersonal offences. The programme of research addressed this objective by designing and conducting studies to:

1. Examine the usability and applicability of BA in the examination, analysis, and interpretation of digital evidence.
2. Examine the ability of BA to contribute to theoretical understanding of the motivational and behavioural dynamics of computer-facilitated interpersonal crimes.
3. Examine the current use and perceived evidential value of BA in policing and law enforcement.
4. Integrate the findings of the preceding objectives into a usable DFIPM that incorporates aspects of BA by identifying the phases and sub-phases required to perform the examination, analysis and interpretation of digital evidence for computer-facilitated interpersonal crimes.

The literature review (Chapter 2) provided a general explanation of the strategies of BA, and its claimed utility in investigating digital crimes (e.g., reduce suspect pool) (Rogers, 2003, Rogers, 2015, Turvey, 2011). It lacked, however, clear explicit steps on how strategies of BA can be applied within the Digital Forensics (DF) investigation process. The researcher sought to investigate the applicability and benefits of incorporating BA within the DF process with the focus on interpersonal offences. The outcome of the studies conducted was then used to identify the phases and sub-phases required to perform examination, analysis and interpretation of digital evidence – designing a behavioural DFIPM that integrates aspects of BA within its phases.

In this regard, the programme of research investigated a number of research questions using appropriate methods. For further clarification and illustration of the direction of the research, the main unanswered questions are listed below.

1. How can BA be applied to the DF investigation process in cases involving the possession and dissemination of Sexually Exploitative Imagery of Children (SEIC)?
2. What does BA contribute to the investigation of SEIC?
3. How can BA be applied to the DF investigation process in cyberstalking cases?
4. What does BA contribute to the investigation of cyberstalking?
5. How can BA be integrated in the DF investigation process?
6. To what extent are DF investigators aware of BA?

7. What perception do DF investigators hold with regard to the use and utility of BA in DF investigations?

3.3 Research Methodologies

Saunders and Tosey (2012) classify research methodology into a five-layer "Research Onion" structure which describes different layers and perspectives on research methodology. The outermost layer represents general research philosophies/paradigms, and their implications for research design. This layer helps identify/select a research model on which the research is based (e.g., positivist, interpretive, critical, pragmatic). The second layer refers to the methodological choices related to specific decisions about utilising a qualitative, quantitative, or a mixed methodology. The third layer concerns the specific strategy that the researcher adopts in order to answer the research question (e.g., survey, action research), while the fourth layer considers the time horizon available in which the researcher needs to address the problem (e.g., cross-sectional, or longitudinal). Finally, the core of the research onion highlights the techniques and procedures undertaken to conduct the research.

For simplicity, Figure 3.1 represents the research onion in a hierarchal structure with the outermost layer at the top, and the core at the lowermost level. It also provides examples of the different strategies that each layer offers.

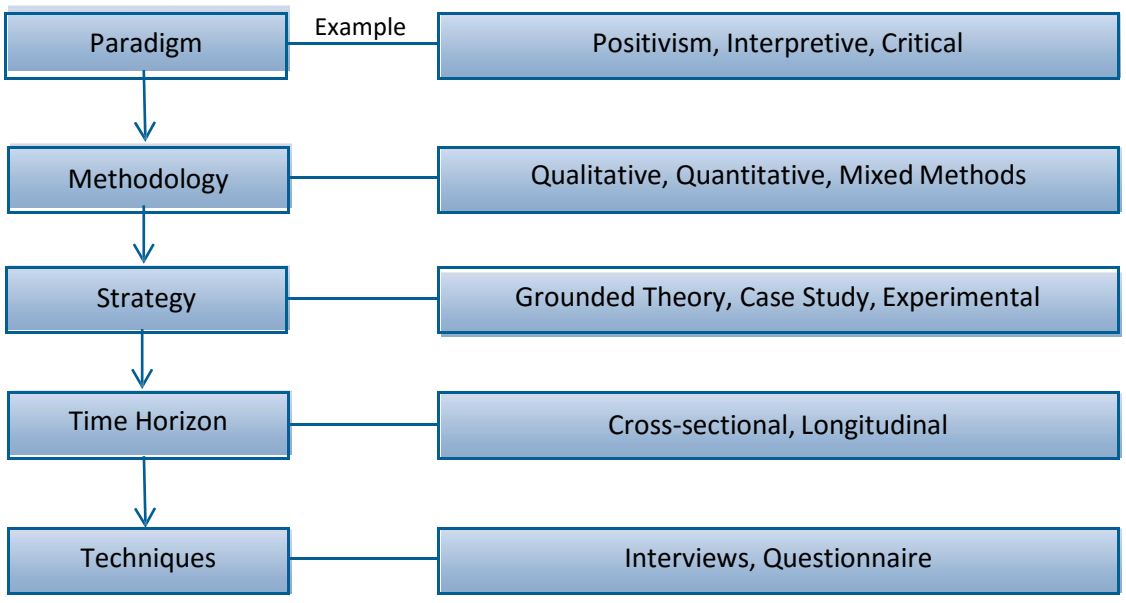


Figure 3.1 A hierarchal representation of the Research Onion

3.3.1 Research Paradigm

Research paradigms refer to the philosophy of the researcher in developing and corroborating their knowledge (Saunders et al., 2009). It is a "worldview"; a framework of perceptions, values, and methods within which the research is conducted. The researcher's view of what constitute acceptable knowledge and the process by which to undertake the development of this knowledge influences and shapes the research design used (Saunders and Tosey, 2012). As such, it is important to select an appropriate paradigm to address the main research questions, and justify the inherent methodology and processes being used.

3.3.1.1 Positivist

As a philosophy, positivism adheres to the view that the world's reality is separated from the researcher's perspectives and beliefs (Saunders et al., 2009). The positivist researcher usually follows a highly structured methodology and depends on large samples of quantitative data that can be analysed statistically to confirm or refute a hypothesis (Saunders and Tosey, 2012). If the hypothesis is refuted, it will be revised and refined then tested by further research. In terms of research methods, the designs used for obtaining data about the objects of study in positivist approaches use a number of methods including laboratory experiments, survey and field experiments (Saunders, 2015).

An advantage of positivism lies in the fact that the strategies it adopts (e.g., large sample sizes, structured procedures, statistical analysis) minimise bias and increase reliability (Chen and Hirschheim, 2004, Gable, 1994). It also enables the replication of the study in different populations which promotes generalisation (Aliyu et al., 2014). A main drawback in positivism, however, is in its objectivity and empiricism which makes it unsuitable in research that tests human behaviour (Aliyu et al., 2014, Houghton, 2011). Also, it provides a general explanation of a phenomenon which can be too abstract to apply to a specific context (Johnson and Onwuegbuzie, 2004). Finally, positivism mainly works with measured variables, calculations, and statistics, which highly constrains the flexibility of its methods (Aliyu et al., 2014).

3.3.1.2 Interpretive

The interpretive paradigm emphasises the relationship between social, cultural, political, economic, and contextual concepts. An interpretive researcher works on understanding a phenomenon through a direct observation of peoples' words, actions, and records in their natural environment (Neuman, 2011). This approach analyses and interprets the collected data to find patterns of meaning related to the topic of interest and research questions addressed with an emphasis on the context and understanding the complex nature of human behaviour. Interpretive researchers mainly depend on qualitative approaches in order to produce detailed descriptions of participant behaviours, rather than using quantitative mathematical analysis

(Bryman, 2015, Saunders et al., 2009). Their methodological choices include case studies, ethnography, grounded theory, and participant observation (Choudrie and Dwivedi, 2005).

The strength of the interpretive approach comes from the fact that it appreciates the complexity of human nature, action and behaviour, and understands that it cannot be quantified or measured mathematically. As such, it attempts to explore and understand a specific phenomenon without excluding the complexity and context. The interpretive paradigm has been criticised for lack of generalisability of results due to the use of small sample sizes (Orlikowski and Baroudi, 1991). Also, unlike positivism, it lacks a precise scientific methodology. This provides unnecessary flexibility for the researcher, which can be a disadvantage for inexperienced researchers (Silverman, 2013). This, however, happens when the researcher's personal biases, background, experience, and assumptions influence the outcome of the study (Silverman, 2013).

3.3.1.3 Critical

The critical paradigm is a newer theory which has become an alternative to the conventional positivist and interpretive paradigms (McEvoy and Richards, 2006). It employs critical and evaluative strategies that aim to challenge a social phenomenon rather than to explore it (Choudrie and Dwivedi, 2005, Orlikowski and Baroudi, 1991). It is flexible enough to allow the use of qualitative, quantitative, or a mixed methodology in order to explore and challenge the phenomenon in question, and identify better or alternative solutions (Hussain et al., 2013). It places a strong emphasis on power, inequality and social change. Also, unlike the positivist approach, it assumes that society can never be truly studied objectively, but should be studied with an aim to expose flaws and provoke social change (Hussain et al., 2013).

Unlike positivist and interpretive paradigms, the critical paradigm research does not end at passive observation, understanding or interpretation. It also aims to criticise and change relationships, conflicts, and contradictions that the researcher deems restrictive and alienating (Asghar, 2013, Oates, 2005). The nature of the critical paradigm, however, places a greater responsibility on the researcher when it comes to analysing and interpreting the collected data. As people can have different interpretations of a single piece of data, the researcher must be very careful with their assessment and interpretations (Asghar, 2013).

3.3.1.4 Pragmatic

The pragmatic paradigm is associated with action, intervention, and constructive knowledge (Goldkuhl, 2012). It lends itself to multiple realities as it believes that there are different ways to interpret the world and understand a phenomenon (Goldkuhl, 2012). It recognises that a single view cannot be thorough in understanding a phenomenon and thus acknowledges the use of mixed methods in the same research inquiry (Saunders, 2015). It focuses on the research

question and aims to make practical choices in terms of selecting methods that can appropriately address the different angles of the problem under investigation (Creswell and Creswell, 2017). As such, it provides the flexibility to utilise a mix of qualitative and quantitative methods to answer questions that cannot be fully addressed using a single method.

A major strength of the pragmatic paradigm comes from combining multiple methods (i.e., qualitative and quantitative), which can provide triangulation of data, build a rich and in depth insights of a phenomena, and develop a substantial theoretical contribution (Creswell and Creswell, 2017, Venkatesh et al., 2013). The use of mixed-methods, however, places a greater effort on the researcher in terms of integrating the findings of the different methods used, and presenting them in a meaningful manner (Creswell and Creswell, 2017).

3.3.2 Methodology

3.3.2.1 Qualitative

Qualitative research approaches provide a rich and deep insight into a specific phenomenon in its natural settings (Denzin and Lincoln, 2000, Silverman, 2016). It performs in-depth studies on a small sample group in order to explore and understand a specific issue in order to identify core ideas and theoretical concepts to guide the construction of a hypothesis (Atieno, 2009, Silverman, 2016). Qualitative research can be conducted using a number of strategies such as interviews, case studies, grounded theory, focus groups, and ethnography (Silverman, 2016). The collected data is then analysed by sorting and categorising them into patterns. Techniques such as thematic analysis and content analysis may be used to identify themes and patterns that aid in the generation of a hypothesis (Patten, 2017, Silverman, 2016).

A major drawback of qualitative research is the substantial length of time required to complete data collection and analysis (Creswell and Creswell, 2017). Due to this, the researcher does not use a random and representative sample, but rather a smaller, purposeful sample (Atieno, 2009). Also, the quality of the research is largely based on the skills of the researcher and can be influenced by their personal perspectives and biases. On the other hand, qualitative research is good at managing and analysing data without reducing its complexity and context (Denzin and Lincoln, 2000). It looks deeper into an issue and provides in depth, detailed outcomes. Unlike quantitative methods, it is not limited to rigidly definable variables, but addresses complex phenomenon that cannot be understood by quantitative measures (Denzin and Lincoln, 2000).

3.3.2.2 Quantitative

Quantitative approaches are concerned with testing a theory through empirical research composed of measured variables and hypotheses that are analysed with statistical methods (Creswell and Creswell, 2017). This method can be useful in research where there is a large

sample group, variables that can be effectively measured and compared, and where statistical analysis can be employed (Creswell and Creswell, 2017). The researcher aims to address the research problem by finding causal relationships between measured variables to confirm or refute a predefined theory or hypothesis (Patten, 2017). In this methodology, data is usually collected through questionnaires or experimental designs. In its simplest form, statistical analysis of the collected data uses descriptive (e.g., mean, median, standard deviation) and inferential statistics (e.g., ANOVA, correlation and multiple regression).

The power and strength of quantitative research is derived from its employment of strictly scientific procedures, which reduces bias and erroneous conclusions (Walker, 2005). Having a large sample group, researcher objectivity, and the use of precise measuring tools also adds to the quality of quantitative research (Choy, 2014, Johnson and Onwuegbuzie, 2004, Walker, 2005). On the other hand, the literature also identifies a number of disadvantages associated with quantitative research methodologies. The nature of this approach produces results that fail to explain the reasons behind the behaviours and actions of its subjects (Atieno, 2009, Johnson and Onwuegbuzie, 2004). This is because reduction of data to numbers strips it of contextual factors that help interpret the results or explain variations in behaviour within groups of individuals of similar characteristics (e.g., demographic characteristics) (Choy, 2014). Another disadvantage is that the sample group used in quantitative research may share characteristics that do not apply to the general population, which creates potential bias in the research and affects its generalisation (Choy, 2014). Quantitative research requires large sample groups to provide efficient results, which in some cases can be hard to obtain due to lack of resources (Choy, 2014).

3.3.2.3 Mixed-Methods

Given the strengths and weaknesses found in each of the previous methodologies, elements from qualitative and quantitative methods can be combined in a single study design to complement each other, yield comparable data, and provide more confirmatory conclusions (Creswell and Creswell, 2017). This form of inquiry was covered comprehensively by Tashakkori and Teddlie (2010), providing an extensive overview of this method and surveying different approaches and viewpoints to employing it. Many published journal articles and books have supported and encouraged this approach as being effective in a variety of disciplines including social sciences, information systems, nursing, and education (Bryman, 2006, Creswell and Creswell, 2017, Gable, 1994, Johnson and Onwuegbuzie, 2004).

Mixed-methods research is associated with the critical paradigm, which is based on the claimed value of combining characteristics of qualitative and quantitative methods to reach an understanding of a particular issue (Shannon-Baker, 2016). It works on addressing a specific

phenomenon by utilising all the data sources available. While single approach studies can address single type of questions (e.g., explanatory, exploratory), a mixed-methods approach can address a variety of exploratory and confirmatory questions (Creswell and Creswell, 2017, Teddlie and Tashakkori, 2011). This provides greater understanding of complex aspects of the issue investigated that would otherwise not be possible using a single approach alone (Creswell and Creswell, 2017, Shannon-Baker, 2016). The use of mixed-methods, however, increases the complexity of the research design requiring a careful analysis of the type of information provided by each employed method (Venkatesh et al., 2013). The researcher should also consider the strengths and weaknesses of each utilised method. This will also require more time and resources to plan and implement this type of research.

3.3.3 Research Strategy

Research strategy relates to the use of specific data collection and analysis methods to address the questions of the research and reach to a specific conclusion (Saunders, 2015). There are various research strategies employed by researchers in the fields of DF, and the social sciences more generally. Examples of these approaches are: (1) grounded theory, (2) case studies, (3) action research, (4) ethnography, (5) experiments, and (6) quasi-experimental. This section explains each approach and discusses its strengths and limitations.

3.3.3.1 Grounded Theory

Grounded theory is a strategy that is usually used in order to develop a theory from the collected and analysed data (Glaser and Strauss, 2009, Saunders, 2015). It analyses this data and searches for relevant thematic patterns in order to develop a theory, which would then be further tested to confirm or refute it. It implements a qualitative approach, and seeks to study a phenomenon empirically resulting in the formation of focused and abstract theories (Saunders, 2015). For example, data gathered from an interview is transcribed and coded, and then analysed to identify common themes exhibited between participants. As such, theories are developed from the results of the research, rather than examining data to establish whether it fits with a pre-existing theory (Saunders, 2015). This approach has been acknowledged and widely adopted in DF, information systems, and cybercrime research (Ahmad et al., 2012, Alanazi and Jones, 2017, Carlton, 2007, Carlton and Worthley, 2009, Yang and Tate, 2012).

Grounded theory offers great flexibility, but raises concerns when it comes to novice researchers (e.g., difficult to prevent researcher induced biased) (Chong and Yeo, 2015). Potrata (2010) suggested that while experienced researchers can benefit from the flexibility offered by grounded theory, less experienced researchers must follow stricter guidelines. The coding process and the level of detail in this strategy can also be overwhelming to first timers (Goulding, 1999). It is also argued that grounded theory is not suitable for areas where

extensive empirical research has already been conducted (Chong and Yeo, 2015, Goulding, 1999). In such a case, the results from the study can be influenced by previous research and not truly grounded in the data (Chong and Yeo, 2015).

3.3.3.2 Case Studies

Case study research uses exploratory analysis of a single unit (e.g., a person, a group, a phenomenon) within its real life context in order to establish its main features and answer specific questions (Bryman, 2015). When conducting a case study, the researcher is expected to apply their analysis skills, knowledge and reasoning, and then draw conclusions based on what they find (Kardos and Smith, 1979). It is a strategy used to understand complex issues where contextual conditions of the phenomenon being studied are of importance. It is richly descriptive as it employs multiple sources of information (e.g., participants' quotes, archived documents, observations, narratives composed from original interviews) to investigate and understand the issue of interest (Hancock and Algozzine, 2015). Also, while conducting an in-depth investigation of the topic, the researcher gets the opportunity to explore additional questions that may arise (Hancock and Algozzine, 2015). This can result in the formation of new hypotheses that help structure future research, thus advancing the field's knowledge base. Case studies have been adopted in many research areas including DF (Boyd and Forster, 2004, Cahyani et al., 2016, Martini and Choo, 2014, Mohtasebi et al., 2011, Teing et al., 2017).

Despite the wide adaptation of case studies in a variety of disciplines, it has been subjected to a number of criticisms. The lack of methodological guidelines for conducting case studies is one of the major criticisms of this strategy (Willis, 2014). The complex nature of the collected data encourages different interpretations, which can lead to researcher bias (Cornford and Smithson, 2006). There is also the issue of generalisation. As the case study usually depends on a single case, or a very small sample, it provides very little basis for generalisation (Zainal, 2007).

3.3.3.3 Action Research

This strategy mainly denotes learning by practicing. In other words, the researcher gets involved with practitioners in the field that is being studied, rather than treating practitioners as subjects or objects of study (Saunders, 2015). It differs from other strategies in that it focuses on promoting change in the subject studied, and applying knowledge learned elsewhere. The researcher, therefore, diagnoses the situation, plans, takes action, and evaluates, with the involvement of the practitioners (e.g., employees of a specific organisation) (Saunders, 2015). The research process is described as a loop or circle process (Baskerville, 1999). It goes through a number of stages starting by identifying the problem, then planning, acting, and finally evaluating the results (Baskerville, 1999, Baskerville and Wood-Harper, 2016, Stringer, 2013). If the results are satisfactory, then the target is achieved and the loop stops, otherwise the

process is continued until a satisfactory result is obtained (Baskerville and Wood-Harper, 2016, Stringer, 2013).

Similar to other strategies, action research is not without its limitations. As a qualitative research strategy it is criticised for lacking scientific rigor, being lengthy and descriptive, and missing a generally accepted criteria for evaluation (Baskerville, 1999, Baskerville and Wood-Harper, 2016). As this strategy requires the practical involvement of the researcher in studying the issue of interest (e.g., organisational management), it can risk the researcher getting over-involved in the area (Rapoport, 1970) and draw them away from the main purpose of the research. This, however, can be avoided by having well defined boundaries for the research (Avison et al., 2001).

3.3.3.4 Ethnography

This is a qualitative strategy for collecting data that is used to examine complex cultural phenomena. It involves collecting detailed observations of the subject under study in its natural setting for long periods of time to produce rich insights into people's views and actions (Saunders, 2015). This type of strategy investigates a limited number of cases with an aim to explore the nature of the case, rather than to test a hypothesis about it (LeCompte and Schensul, 1999). It uses observation as the main method to collect data; however, interviews can also be used to clarify the researcher's observations (LeCompte and Schensul, 1999). Ethnography differs from other scientific methods (e.g., experiments) as ethnographic researchers do not have control over the field settings, the variables, or the circumstances while studying a specific phenomenon. People's behaviours and circumstances can change over time generating different results, which the researcher must provide clarification for (LeCompte and Schensul, 1999). Ethnography has been applied to published work in the fields of DF and cybercrime (Altiero, 2015, Danquah and Longe, 2011, Steinmetz, 2014, Tow et al., 2010).

Ethnography has been criticised in relation to the process of conducting the research. It lacks a systematic way to conduct the fieldwork and collect data (Hammersley and Atkinson, 2007). It has also been argued that results are unrepresentative and cannot be generalised due to the small sample size (Hammersley and Atkinson, 2007). This research methodology also generates a large amount of data that needs to be analysed, organised, and structured into coherent presentation (Fetterman, 2010). Also, the research depends on the skill and rigour of the researcher and is often hard to replicate (Fetterman, 2010, Hammersley and Atkinson, 2007).

3.3.3.5 Experiments

In its simplest form, an experiment examines the relationship between two (or more) variables to identify whether a change in an independent variable causes a change in a dependent variable

(Patten, 2017). It also measures the size of change and the significance of the influence of the independent variables (Saunders, 2015). It aims to test a hypothesis by manipulating the variables of interest in a controlled environment to produce more definitive conclusions regarding the relationship between the variables (Patten, 2017). The nature of the experimental strategy provides the researcher with a high level of control over the variables. This raises the confidence of the researcher when drawing conclusions as to whether the change in one or more factors affects the outcomes (Christensen et al., 2011). It is also a straightforward scientific approach that can be easily applied to a variety of disciplines (Christensen et al., 2011). Experiments have been adopted in many DF and cybercrime studies (Al Sharif et al., 2014, Atefi et al., 2014, Graves et al., 2014, Marziale et al., 2007, Roussev and Richard III, 2004).

Experiments also have their drawbacks. Conducting the research in a highly controlled environment (e.g., laboratory) creates an artificial situation which cannot be fully realistic and does not represent real-life environments (Saunders, 2015). Also, despite the preconception that experiments (i.e., scientific method) are free of human subjectivity, they are still constructed by a human and prone to error and bias (Christensen et al., 2011).

3.3.3.6 Quasi-experimental

The prefix *quasi* means "resembling'; denoting that quasi-experimental is a research strategy that resembles, but is not a truly experimental study. This strategy employs a number of aspects of experimental design (e.g., testing a hypothesis), yet the researcher has limited control over the assignment of subjects (Levy and Ellis, 2011). Instead of being selected randomly, subjects are assigned out of convenience to the study to be conducted (Levy and Ellis, 2011). Quasi-experiments are usually employed in field settings to study variables that would be impractical, unethical, or difficult to manipulate (Campbell and Stanley, 2015, Levy and Ellis, 2011). These are easier to design compared to true experiments. They do not require the establishment of well-controlled laboratory settings, which reduces their vulnerability to criticisms of external validity. Quasi-experiments have been adopted in many research areas including DF, cybercrime, and cyber security (Daryabar et al., 2016, Grispos et al., 2014, Ivaturi et al., 2017, Tang et al., 2013).

Despite the advantages of quasi-experiments, the lack of random assignment of subjects increases the risk of affecting the internal validity of the study (e.g., effect of selection). There is also the problem of the influence of unmeasured or confounding variables which can affect the outcome of the study (Campbell and Stanley, 2015). Two examples of these are history and maturation. History refers to having other current events influence the change in the dependent variable, while maturation involves having normal developmental process cause change in the dependent variable (Campbell and Stanley, 2015).

3.4 Methodology Selection and Rationale

For this research the pragmatic paradigm was identified as being the most appropriate. This is because the research sought to answer different questions related to understanding offender/victim's behaviour through digital evidence, examining the utility of BA in investigating specific types of digital crimes (i.e., computer-facilitated interpersonal crimes), and proposing a *practical* model to complement the standard DF investigation process. The researcher needed to first assess the utility of implementing aspects of BA within the DF investigation process for two types of computer-facilitated interpersonal crimes. This also constituted a critical examination of what BA adds to the investigation that the standard DF investigation process lacks. Also, part of the success of implementing BA within the DF process highly depends on the perspectives of the individuals affected (i.e., DF practitioners). The research aimed to measure practitioners' perceived utility of BA, which provides an indication on the level of acceptance to incorporate this approach. It also aimed to identify factors that prevent DF practitioners from utilising BA within DF investigations, in order to design solutions. The development of the DF investigation model and the interpretation of the digital evidence, however, had to be objective in some respect. As such, the research was approached from a pragmatic perspective in that there were multiple realities to be understood in an effort to assess the utility and implementation of BA within the DF process.

As such, a mixed-methods approach was implemented in the programme of research as this was most suited to the objectives and research questions. The complex nature of this research makes the use of a single qualitative or quantitative approach inadequate to fully examine the issues under investigation. The combined methodology provided more insight into the research problem and an expanded understanding of the issue. The multidisciplinary nature of the research also created challenges in using one specific methodology for all the studies undertaken. As a result, the research adopted a variety of designs depending on the aims and research questions of each specific study.

Since the research mostly dealt with variables that were hard to measure and quantify (e.g., offender behaviours, motivations, victim risk factors), the positivist paradigm would not be a suitable base theory from which to build the research. As this paradigm is totally objective and relies mainly on hard facts and numbers, it would fail to consider the contextual factors that play a role in human behaviour when investigating computer-facilitated interpersonal crimes. Using this paradigm would also result in an outcome that lack an in depth understanding of the possible utilities of BA in investigating these crimes, and how it can be implemented within the standard DF investigations.

The interpretive paradigm would not be appropriate as this research does not aim to only observe, explore, and understand current DF practices. It seeks to extend the current practices by proposing a pragmatic DFIPM that would assist the DF investigation of specific types of computer-facilitated interpersonal crimes.

3.5 Study 1 (Investigative/Exploratory)

Study 1 employed a mixed-methods approach with quantitative and qualitative analysis of relevant digital evidence and case documentation. This design was most appropriate for this study given the time constraints and limited amount of resources (i.e., cases). The study aimed to investigate the utility of BA during the DF process of two types of computer-facilitated interpersonal crimes: SEIC and cyberstalking. For each type of crime, a selection of archived cases was obtained from Dubai Police. Each case was examined and analysed individually using the standard DF procedure (Casey, 2002), and strategies of BA as applicable. The examination produced qualitative data that was analysed using thematic analysis (e.g., offender motivation reflected by the digital evidence). All case related documents were also analysed (e.g., background of offence, interview scripts). For example, interview scripts of SEIC offenders were analysed thematically to understand their motivation for offending. Descriptive statistics were also used to analyse the demographic data of offenders and victims, and the involved offending behaviours.

It is important to note that the researcher investigated each individual case *afresh*, without knowing the identity of the offender (unless it was mentioned in the police request letter). The researcher did not review the original report that included the results of examination and analysis of each case prior to conducting the DF investigation. This was to ensure that the investigation process used by the researcher was not influenced or guided by the original results from the case documents. As such, the original results were only reviewed *after* the researcher concluded the case analysis in order to compare the findings.

Study 1 was performed in two parts and is reported in two separate chapters. Chapter 4 covers testing the utility of BA for the DF investigation of SEIC cases. Chapter 5 covers testing the utility of BA for the DF investigation of cyberstalking cases. Sections 3.5.1 and 3.5.2 describe the study design and analysis performed for each part of the study.

3.5.1 Testing the Utility of Behavioural Analysis in the Digital Forensics Investigation of SEIC Cases – Study Design

This study explored how BA can be applied within the novel context provided by the digital environment in SEIC cases. It mainly focused on examining the ability of BA to assist in

understanding the motivational and behavioural dynamics of computer-facilitated interpersonal offences, and aid in the interpretation of associated digital evidence. Thus, the main research questions addressed were the following:

1. How can BA be applied to the DF investigation process in SEIC cases?
2. What does BA contribute to the investigation of SEIC?
3. What are the characteristics of SEIC offenders?
4. What motivates SEIC offenders?
5. How do SEIC offenders justify their behaviour?

The study used an abductive approach that followed the standard digital forensics process to analyse individual cases separately and applied strategies from BA. It specifically focused on applying the four strategies of Behavioural Evidence Analysis (BEA); a subset of BA, (i.e., equivocal evidence analysis, victimology, crime scene characteristics, and offender characteristics) to the examination of each case. These strategies were described in Chapter 2.

The study was conducted at the secured labs of the Department of Electronic Evidence - General Department of Forensic Science and Criminology – Dubai Police. The data that was used in this study were duplicated copies (known as "bit-wise images" in the digital forensics field) of the contents of the digital media devices (e.g., mobile phones, computers, hard-disk drives, memory cards) that were seized in criminal cases by Dubai Police. The acquired images of these devices can contain "evidence" that supports the case, including digital files (e.g., documents, pictures, log files, history files, emails, contact lists). Initially, three to five cases per crime were to be analysed depending on the amount of evidence available per case. These were forensically examined using BA to identify behavioural patterns, motivations, and characteristics of offenders and victims. The examined cases were committed in Dubai between 2009-2013. An analysis workstation, as well as the DF hardware and software required for the study (e.g., EnCase, AccessData, sanitized hard-disk drives, write-blockers), were provided by Dubai Police and used to conduct the examination and analysis. The study also produced qualitative data related to offender motivations and justifications for their behaviour, which was analysed using thematic analysis where applicable.

3.5.1.1 Test Environment and Requirements

For the purpose of conducting the study, several hardware and software tools were used. Two Dell Precision PWS 490 workstations with Intel® Xeon® CPU X5365 @ 3.00GHz, 3.25GB of RAM, Microsoft Windows XP Professional, and a 300 GB hard-disk formatted with NTFS were set and configured at the secure lab of the Department of Electronic Evidence – General Department of Forensic Science and Criminology – Dubai Police. The workstations were up to date with all the necessary security patches and updates. The tools required for conducting the

study and analysis were installed, configured and verified. The workstations were secured with passwords and were isolated from the lab's network, as well as any other connection (e.g., blue tooth, wireless). The following is a list of all the other hardware and software tools that were used throughout this phase:

1. Two sanitized portable hard-disk drives (1TB and 3TB).
2. TextPad version 4.5.2.
3. EnCase version 6.5.
4. Access Data Registry Viewer.
5. Inex.dat Analyzer v2.5.
6. MozillaCacheView and MozillaHistoryView.
7. ChromeCacheView

3.5.1.2 Cases Selection and Sample Size

The researcher followed convenience sampling, which is a non-random sampling technique where subjects are selected due to practical specifications such as accessibility and readiness to be part of a sample at a given time (Etikan et al., 2016). This strategy was chosen as it provided a practical and economical method to collecting the required data, given the time constraints of completing each study, and the limited number of cases available for each category of crime. The selection of the sample cases, however, had inclusion criteria based on offender behaviour which met the definition of SEIC (see Chapter 2), use of a Windows-based computer as the main offending platform, the availability of image files (acquired bit-wise images of the contents of the digital devices seized), and the availability of interview scripts with offenders/victims. Initially, five cases of offences were selected from the digital crime cases archive at Dubai Police. All the image files of the seized devices for each case, as well as all related documents (e.g., background of the offence, interview scripts, information about the offender), were copied and analysed during the study.

The sample size for the study was based on analysis of a number of cases to adequately answer the research questions. That is, until new categories, themes or explanations stop emerging from the data (Glaser and Strauss, 2009). It was initially intended that five cases would be analysed. However, as the examination and analysis developed the researcher felt the necessity to add more cases. The total number of the sample cases was 15.

3.5.1.3 Data Sources

The primary data source for this study was the electronic data (e.g., documents, images, videos, registry keys, Internet cache and history files, metadata of files) stored on the image files of the seized devices for each case. Depending on the case, the image files covered devices that ranged

from desktop computers and laptops to smart phones and memory cards. Data obtained for each case also included documents detailing the background of the case (e.g., a detailed description of the offence, the offender, and the seized digital devices, and interview scripts with the offenders or witnesses). Since this study aimed to apply BA strategies, understanding the context of each case was a crucial step prior to analysing the associated evidence. Thus, for each case, all the available supporting documents were carefully studied before starting to analyse the image files.

3.5.1.4 Data Collection

The data collection used in this study combined the technical skills of DF analysis and the analytic skills of BA. The technical skills were required to identify sources and traces of evidence required in digital crime investigations. The BA strategies were important to understand the behavioural dynamics and the *context* of the crime. Understanding the context in a crime aids in having better interpretations of the circumstances surrounding the crime, and can identify key facts in the investigation (Rogers, 2015, Rogers and Seigfried-Spellar, 2014).

Data collection started on the 24 August 2014 at the Department of Electronic Evidence – Dubai Police. In the SEIC category of crime, the DF practitioner usually receives the suspect's seized digital devices from the requesting party (e.g., Criminal Investigation Department (CID), Police station). As such, the examination of the devices attempts to reconstruct the suspect's activities in obtaining and sharing the files, therefore, answering the questions of what, why, where, and how the suspect had obtained them. In all of these cases, there were identified suspects. Therefore, BA was not used for the purposes of identifying and locating a totally unknown offender, but to help in the investigation process in other ways (e.g., identify evidence that reflected the offender's intentional engagement in downloading SEIC, identifying the actual offender in the case).

To answer the main research questions for this study, a number of sub-questions were defined for the examination and analysis phase for this category of offence. The first set of questions aimed to identify *technical* evidence to support the case (i.e., to support the hypothesis that the offender had committed the offence(s) for which they had been charged). For each case examined in this study, the analysis addressed questions related to offender behaviour and offence dynamics. These questions were primarily *content* based (except if indicated otherwise); focusing on technical artefacts to inform the case, and were organised around the following topic areas:

1. In cases where the offender owns multiple digital devices, where are SEIC more likely to be stored?

2. What are the most common locations of potential evidence files (in terms of folders and directories)?
3. What means does the offender use to obtain SEIC (*modus operandi*)? (primarily context)
4. What evidence proves the knowing download of SEIC?
5. What evidence proves the sharing of SEIC?
6. What traces/artefacts show that files of interest have been deleted?
7. In cases where no intact SEIC files are found, what other evidence can suggest that the offender attempted to download these files?

The second set of questions aimed to identify offender characteristics, understand their behaviour, and the circumstances surrounding the crime. This set of questions was primarily *context* based (except for the first three items) and was organised around the following subjects:

1. What are the demographic characteristics of the SEIC offender?
2. What is the approximate volume of the downloaded/shared SEIC files?
3. Is there evidence of the possession of other paraphilic imagery (e.g., adult pornography, bestiality, fetishism)?
4. What is the offender's motivation(s)?
5. What justifications does the offender provide for their behaviour?
6. How are the SEIC files sorted/categorised?
7. Does the offender communicate online with other SEIC offenders?
8. Is there evidence of suspicious online communications between the offender and minors?
9. To what extent does the offender employ anti-forensic skills to evade detection (e.g., hide/wipe evidence, use of anonymous web browsing).

After carefully studying all of the related documents for each case to understand the related context, the DF examination phase started. During the examination of some cases the researcher needed to revisit steps in light of a more refined understanding of the case. The findings in each case were collected to be further processed in the Data Analysis section (Section 3.5.1.5).

Although the process described in this section appears to be linear, in practice the steps of the DF investigation and BA cannot be clearly separated. They are most often intertwined, and the DF investigator may find it necessary to revisit steps in order to find more evidence and develop a better understanding of the case.

3.5.1.5 Data Analysis

The collected data for each case was summarised, and similar patterns identified in different cases (e.g., locations of evidence, method to obtain SEIC, means used to evade detection) were grouped together. The first stage of the analysis focused on identifying the location of all potential sources of digital evidence in a post-mortem forensic examination.

The second phase identified offender characteristics and motivations, with relevant data sources and evidence being examined on a number of parameters:

1. Sociodemographic variables: age, ethnicity, professional status, marital status, and number of children.
2. Criminological variables: motivation, criminal history, and types of prior offences.
3. Psychosexual variables: estimated volume of downloaded material, the format of the files in possession (e.g., images, video, written stories), and the possession of other paraphilic materials (e.g., bestiality, fetishism).
4. The anti-forensics skills and sophistication of the offender as reflected by the use of countermeasures to conceal files or hide traces of their illegal downloading of these.
5. Classifying offenders based on the recovered evidence as producers, traders, viewers, downloaders, and sharers; as adapted from typologies identified in the literature review (Chapter 2).
6. Other child pornography related activities including the method of obtaining the files of interest, as well as sorting and categorising of files.

After reviewing the collected data, the researcher had to exclude marital status and number of children as the related data for these variables were missing for the majority of the offenders.

The collected quantitative data was analysed using descriptive statistics. Similar patterns were counted and collated as percentages (e.g., offender demographics, offender category, method of obtaining SEIC). Results are presented in Chapter 4, and are discussed and compared to findings of previous research.

The collected qualitative data (e.g., interview scripts) was analysed using Thematic analysis (Braun and Clarke, 2006). The researcher coded the data and identified themes associated with the objectives of the study (e.g., offender justification for their behaviour). The analytic process followed the stages outlined and utilised by other researchers (e.g., (Braun and Clarke, 2006, Bryce and Fraser, 2014)). The initial stage of analysis involved the comments in the dataset being read a number of times in order to achieve familiarisation with the data, and to develop a list of coding labels associated with the statements. This was followed by initial coding and organisation of the data (Robson, 2011). An iterative review process of coding and

identification of themes was then undertaken to ensure the accuracy and consistency of the analysis (Braun and Clarke, 2006).

3.5.2 Testing the Utility of Behavioural Analysis in the Digital Forensics Investigation of Cyberstalking Cases – Study Design

This study followed the same design described in Section 3.5.1 for testing the application and utility of BA with SEIC cases. It explored how BA can be applied within the novel context provided by the digital environment in cyberstalking cases. The study used an abductive approach that followed the standard DF investigation process to analyse individual cases separately applying the four strategies of BEA; a subset of BA, (i.e., equivocal evidence analysis, victimology, crime scene characteristics, and offender characteristics) to the examination of each case. These strategies were described in the Literature chapter (see Section 2.2.6).

It examined how strategies of BA can be utilised to infer motivational and behavioural dynamics from the associated digital evidence. As such, the main research questions addressed were the following:

1. How can BA be applied to the DF investigation process in cyberstalking cases?
2. What does BA contribute to the investigation of cyberstalking?
3. What are the characteristics of cyberstalking offenders?
4. What motivates cyberstalking offenders?

3.5.2.1 Test Environment and Requirements

The study was conducted at the secure lab of the Department of Electronic Evidence – General Department of Forensic Science and Criminology – Dubai Police. For details of the hardware and software used refer to Section 3.5.1.1.

3.5.2.2 Case Selection and Sample Size

The selection of the sample cases followed the same procedure described in Section 3.5.1.2, utilising convenience sampling (Etikan et al., 2016). Inclusion criteria were based on victim experience of offending behaviour which met the definition of cyberstalking (see Chapter 2), use of a Windows-based computer as the main offending platform, the availability of bit-wise image files, and the availability of interview scripts with offenders/victims. For example, the digital devices seized in cases varied (e.g., computers, smartphones, flash drives, etc.). However, as the focus of the study is on computer-facilitated interpersonal crimes, only cases in which computers were the main platform of offending were included in the sample.

The sample consisted of 20 cases that involved different variations of cyberstalking (e.g., false accusations, defamation, extortion), and were committed in Dubai between 2009-2013. These cases involved 31 computers with hard-disk drives capacities ranging from approximately 40GBs to 300GBs of data. The hard-disk drives of all of these computers had been previously acquired, verified and archived by the Electronic Evidence Department at Dubai Police.

3.5.2.3 Data Sources

The primary data source for this study was the electronic data (e.g., documents, images, emails, chat logs, Internet cache and history files) stored on the image files acquired of the seized computer hard-disk drives for each case. Also, for each case, all the related police documents were obtained for analysis (e.g., background of the offence, interview scripts).

3.5.2.4 Data Collection

In this category of crime, the DF investigator usually receives the victims' computers. In cases where there were identified suspects, their computers were also seized for examination. As such, the examination of the devices attempts to reconstruct the communication between offenders and victims, identify the predominant motivation of the offenders, understand the context in which the cyberstalking occurred, and identify the prior relationship between victim and offender.

To answer the main research questions for this study, a number of sub-questions were defined for the examination phase for this category of crime. The set of questions aimed to identify technical evidence related to the case (e.g., identify offender signature behaviour to aid in reducing the suspect pool), to identify offender and victim characteristics, and to understand their behaviour. For each case examined in this study, the analysis addressed questions related to offender behaviour and offence dynamics and were organised in two parts: primarily *content*, and primarily *context*. Questions that were primarily content are as follows:

1. What are the most common locations of potential evidence files?
2. What are the demographic characteristics of the offender?
3. What are the demographic characteristics of the victim?
4. Is the victim the only person being targeted by the offender?
5. What is the criminal history of the offender?

Questions that were primarily *context* are the following:

1. What means did the offender use to cyberstalk their victim (*modus operandi*)?
2. What is the nature of the victim/offender relationship?
3. What behaviours contribute to placing the victim at risk?
4. What might have motivated the offender?

5. What level of risk does the offender pose?
6. To what extent does the offender employ anti-forensics skills to evade detection?

The DF analysis process of the collected data was iterative, and progressive. The two frameworks; digital forensics (traditional examination and analysis phases) and BA, complemented each other and were performed concurrently. For each case, the extracted digital evidence at each step was used as input to BA, and the output was used to provide direction to additional locations of potential evidence, provide insights on offender/victim behaviour and characteristics, and further inform the investigation process.

3.5.2.5 Data Analysis

The findings of the analysis for each case were summarised, and similarity in data sources, interpretation and characteristics grouped together.

The set of questions in the previous section identified victim and offender characteristics and behaviours, with relevant data sources and evidence being examined on a number of parameters:

1. Sociodemographic variables: age, gender, ethnicity, employment status, marital status, qualification, and computer literacy.
2. Criminological variables of the offender: motivation, criminal history, types of prior offences, and psychiatric history.
3. Variables related to the offending behaviour: the length of the online harassment, means of contact (e.g., email, personal chat service, social networking sites, forums and bulletin boards), type of harassing behaviour (e.g., identity theft, use of imagery, proclamation of love, sexual comments, threats and violent comments, and defamation).

After analysing the collected data, the researcher had to exclude the offender's psychiatric history, marital status and computer literacy variables as this data was unavailable for the majority of the offenders.

The collected quantitative data was analysed using descriptive statistics. Similar patterns were counted and collated as percentages (e.g., offender demographics, victim demographics, method of cyberstalking). Results are presented in Chapter 5, and are discussed and compared to findings of previous research.

The analysis of the qualitative data obtained through the forensic device examination and from the investigative files (e.g., cyberstalking communications, interview scripts) was also undertaken using thematic analysis, as described and used by other researchers (e.g., Braun &

Clarke, 2006; Bryce & Fraser, 2014). The researcher followed the same steps described in Section 3.5.1.5.

3.5.3 Reliability and Limitations

In order to assess the reliability and validity of the outcome of the study and to minimise bias, the researcher sought to address four criteria: (1) credibility, (2) transferability, (3) dependability, and (4) confirmability (Lincoln and Guba, 1985). This strategy has been adopted by other scholars to discuss the trustworthiness of qualitative research in information systems (e.g., Gregory et al., 2016). Credibility refers the internal validity of the research; assessing whether the study accurately measures what is intended (Shenton, 2004). It involves a number of strategies which include: the use of appropriate methods, developing familiarity of the research context, random selection of the sample, triangulation, ensuring honesty of the informants when contributing data, qualification and experiences of the researcher, and pear scrutiny of the research project (Shenton, 2004). Transferability refers to the external validity of the research; measuring the extent to which the results of the research can be applied to other situations (Shenton, 2004). It is addressed by providing sufficient description of the context in which the study was undertaken, and the phenomenon under investigation (Shenton, 2004). Dependability assesses whether repeating the work of the research (by other researchers) using the same methods, context, and sample will yield similar results (Shenton, 2004). It is addressed by providing in-depth descriptions of the research design and implementation. Confirmability is associated with objectivity; ensuring that the findings of the study are resulted from the data collected, and are not influenced by the researcher's preferences and perspectives (Shenton, 2004). It is addressed by adopting methods that ensure triangulation, providing clear methodological description that are easy to follow by other researchers, and acknowledging the shortcomings of the study (Shenton, 2004). These terms are used below and also in the Reliability and Limitations Sections for Studies 2 and 3.

Credibility, transferability and dependability of Study 1 were addressed by providing detailed description of the study design, and the procedures followed for data collection and analysis. The use of a mixed-methods approach was utilised to select appropriate procedures that address the different questions of the study. The use of *real* crime cases in testing the applicability and utility of the integrated procedure of DF and BA also increases the credibility of the collected data and the findings, as opposed to the use of fictional scenarios performed in earlier studies identified in the literature (e.g., Silde and Angelopoulou, 2014). The collection and analysis of both qualitative and quantitative data from different case-related sources (i.e., bit-wise image files, case documents, interview scripts of offender(s)/victim(s)) was to achieve triangulation. Performing the study in two parts; using a sample of a different computer-facilitated interpersonal crime category for each part, addresses transferability of the results.

Confirmability is addressed by following a number of strategies to reduce bias in the findings of the study. Confirmability was strengthened by the researcher working with a multidisciplinary supervisory team (having expertise in psychology, information systems, computer engineering, and digital forensics) discussing the different stages of the study design, data collection, and data analysis. Investigating each individual case *afresh*, without reviewing the results in the original case documents also ensured that the findings of the study were not influenced and biased by the results in the original report. The 15 years' experience of the researcher in investigating digital crimes also aided in controlling bias by trying to stay objective through the different stages of investigating the sample cases. Interpretations of the collected evidence (presented in Chapters 4 and 5, Tables 4.4 and 5.6) were further revised by the researcher and the supervisory team to reach the final output. Finally, both parts of the study were peer-reviewed and published in scientific journals (Al Mutawa et al., 2015, 2016).

A number of limitations were identified in the study. Due to practical issues, the study did not use random sampling and instead utilised convenience sampling of the cases. The use of random sampling is argued to provide more assurance with regards to the representativeness of the results (Shenton, 2004). The researcher, however, also identified criteria to the selection of the cases (see Sections 3.5.1.2 and 3.5.2.2) to insure the use of information-rich cases with a variety of data resources. A limitation was also the fact that all of the cases examined in this study occurred in the United Arab Emirates and were obtained from the Dubai Police. This limitation does not, however, diminish the value of analysing the digital evidence in these cases as it adds to what is already established in the literature by other researchers. Also, since similar technology is used for committing these crimes, it is fair to say that the selected cases would be generalisable to other agencies worldwide. The researcher is not aware of any additional non-technological factors in the selected cases which would make them unique to the UAE or otherwise not generalisable.

Finally, despite the small sample size in the study, it provided an insight into a phenomenon that is under-researched. Experimenting with a greater number of SEIC and cyberstalking cases from different countries is required to examine a greater variety of digital evidence that may more effectively reflect the dynamics of the crime, as well as offender and victim behaviours. However, the researcher did not have control over this issue as she was restricted with the cases obtained from Dubai Police.

3.6 Study 2 (Survey)

This study employed an online questionnaire to collect quantitative and qualitative data from a sample of DF practitioners. The study aimed to examine the perceived utility of BA, including strategies of BEA (see Chapter 2), and its implementation within the standard DF process

during the investigation of specific computer-facilitated interpersonal crimes by DF practitioners. It focused specifically on the extent to which practitioners currently use activities that constitute BA in the digital evidence processing stages of SEIC and cyberstalking cases. It also addressed the perceived utility of these approaches to enhance the quality of the gathered digital evidence, and associated challenges in performing these analyses. The questionnaire mainly consisted of quantitative items, and included a small number of related open-ended questions. The participants were DF investigators at both local and international levels recruited through existing and developed contacts with relevant DF agencies. The questionnaire was hosted online for two months, with a target sample of 70-100 participants. Data analysis used descriptive statistics, and the open-ended question data was analysed using thematic analysis. The questionnaire was designed according to best practice recommendations (Draugalis et al., 2008, Kitchenham and Pfleeger, 2002). Results are reported in Chapter 6.

3.6.1 Materials

This section describes the content of the online questionnaire. It had a total of 30 questions with an anticipated answer time of ten minutes. The questions were divided into four sections. The first section asked for demographic information. The second section tested participant awareness of BA; with a specific focus on BEA and its different strategies as described by Turvey (2011). The third section measured the use of BA activities in the DF investigations of SEIC cases, whereas the fourth section measured the use of BA activities in the DF investigations of cyberstalking cases.

3.6.1.1 General Demographics, Training and Experience

This section included a number of items that measured the demographic characteristics of the participants. It consisted of nine closed and partially close-ended questions. These asked the participants about their age, gender, level of education, area of expertise, the country in which they practice digital forensics, and the type of organisation in which they are currently employed. It also asked them to estimate the number and the type (e.g., fraud, hacking, rape, cyberstalking) of criminal cases that they had investigated during their career. Finally, it asked the participants whether they followed a specific methodology when conducting DF investigation in a case. This question used a response category of “yes” or “no”. It also asked them to explain why or why not they followed a specific methodology. Thirteen variables were measured in this section as follows:

1. Gender
2. Age
3. Highest education level
4. Area of primary qualification

5. Training undertaken
6. Country where they practice digital forensics
7. Organisation type
8. Years of experience in the field of digital forensics
9. Number of departments where they have worked in
10. Current job title
11. An estimate of the digital forensic investigations performed
12. Types of crimes investigated
13. Following a specific digital forensics methodology

3.6.1.2 General Awareness and use of BEA

This section measured the factor of awareness of BEA by DF practitioners. It was a short section that consisted of three questions using response categories of "yes" or "no", and one open-ended question. The first question asked participants about their knowledge of BEA. If their response was "no", they were not asked to answer the remaining questions in this section. The second and third questions asked the participants about their knowledge of the strategies which constitute BEA, and whether they had utilised it in a DF investigation. The last question was open-ended and asked the participants for their comments and insights on the utility of BEA for investigating digital crimes. Three variables were measured in this section:

1. Awareness of BEA
2. Awareness of the strategies of BEA
3. Utilising BEA in investigations

3.6.1.3 Behavioural Analysis Use and Utility in Relation to Investigating SEIC Cases

This section consisted of six questions. The first question had response categories of "yes" and "no", and asked participants if they had ever investigated SEIC cases. If their response was "no", they were not asked to answer the remaining questions in this section. The second question asked them to provide an estimated number of the cases they had investigated. The scale of measurement was developed and refined by the researcher and the supervisory team, and ranged between 1-50+ cases. The third question used a Likert scale (Likert, 1932) that aimed to measure the frequency of performing activities that constitute BA when investigating SEIC cases. The construct was measured by six statements, each focusing on a specific activity that constitutes BA (e.g., performing a time line analysis, looking for evidence that reflect the offender's behaviour). These were measured on a 5-point scale (1 = never, 5 = always). The statements were developed by the researcher. An example statement was "I look for electronic evidence that reflects the behaviour of the offender in an attempt to understand their

motivations". A high score indicated a high frequency in performing activities that constitute BA when performing DF investigations on SEIC cases.

The fourth question used a Likert scale (Likert, 1932) that aimed to measure the perceived utility/efficacy of BA. The construct was measured by nine statements each focusing on a specific utility of performing BA when investigating SEIC cases (e.g., provide more knowledge on offender motivation, provide more knowledge on the psychological state of the offender). These were measured on a 5-point scale (1 = strongly disagree, 5 = strongly agree). The statements were developed by the researcher. An example statement was "Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about their motivation". A high score indicated that the participant had a high perceived utility of BA when performing digital forensics investigations on SEIC cases.

The last two questions were open-ended aimed to obtain participants comments on the challenges they faced when performing digital forensics on SEIC cases, and to solicit their thoughts on suggestions to improve the digital forensics investigation of these cases. The main variables measured in this section were:

1. Frequency of digital forensics performed on SEIC cases
2. Frequency performing different activities that constitute BA.
3. Perceived utility/efficacy of activities constituting BA.

3.6.1.4 Behavioural Analysis Use and Utility in Relation to Investigating Cyberstalking Cases

This section consisted of six questions which followed the same structure and measured the same variables as described in the previous section.

3.6.2 Ethical Considerations and Ethical Approval

Pursuant to the University of Central Lancashire policy, the questionnaire and related documentation was submitted to the University Ethics Committee prior to the commencement of the survey. The Ethics Committee granted approval on December 22, 2015 and assigned the survey approval code STEMH 417.

Consistent with the university's policies on research, potential participants were provided with a "Participant Information Sheet" prior to commencing the survey and a "Debrief Information Sheet" at the end of the survey, prior to submitting their responses. Potential participants were advised of the purpose of the study, and the criteria used for selecting participants. They were also informed that participation was voluntary, that all the responses were anonymised, and that

all data are kept confidential. Completing the survey and submitting it indicated participant consent to take part in the study (see Appendix 1).

3.6.3 Procedure and Sampling

The questionnaire was not formally pilot tested due to limitations in time and resources (i.e., DF practitioners willing to take part in the pilot study). However, the questions were reviewed and discussed by the researcher and the supervisory team to agree on a version. Three DF practitioners from the Dubai Police also volunteered to take the questionnaire and provide their comments with regards to the clarity of the questions. Their input was used to further refine the questions and produce the final version.

The questionnaire was hosted on the Survey Gizmo website (https://app.surveygizmo.com) from February 1, 2016 to March 31, 2016. The questionnaire was promoted by sending invitation emails to the potential participants. A link to the questionnaire was provided within the invitation emails. Participants were mainly recruited through the LinkedIn established connections with national and international DF professionals and cybercrime investigators. Invitations were also sent to other existing contacts, whom the researcher had previously met in DF training courses and conferences, work colleagues from the Dubai Police, as well as contacts provided by the supervisory team.

The anticipated potential size of the sample ranged from 70-100 participants. Emails soliciting participation were sent to 877 potential participants. A total of 246 (28.1%) respondents completed the questionnaire. A closer examination of the data, however, showed that 93 entries were incomplete; therefore, they were excluded from the dataset. As such, only 153 (17.4%) completed questionnaires remained for the analysis. Despite this, the sample size had 83 more completed questionnaires over the initial minimum anticipated number. A number of the participants who did not complete the questionnaire reported that their expertise related to fields other than SIEC and cyberstalking, and as such they felt that they would not be able to provide useful information for the survey. Also, it was expected that many of the potential participants are DF investigators with very busy schedules that prevented them from participating in the survey.

3.6.4 Data Analysis

The collected quantitative data was analysed using descriptive statistics. Similar patterns were counted and collated as percentages.

With regards to the open-ended questions Thematic analysis (Braun and Clarke, 2006) was used by the researcher to code the data and identify themes associated with the objectives of the

study. The analytic process followed the stages outlined and utilised by other researchers (e.g., Braun and Clarke, 2006, Bryce and Fraser, 2014). The initial stage of analysis involved the comments in the dataset being read a number of times in order to achieve familiarisation with the data, and to develop a list of coding labels associated with the responses. This was followed by initial coding and organisation of the data (Robson, 2011). An iterative review process of coding and identification of themes was then undertaken to ensure the accuracy and consistency of the analysis (Braun and Clarke, 2006). Relevant quotations were identified during this stage to support the analysis/interpretations of the data.

3.6.5 Reliability and Limitations

The credibility, transferability and dependability of the results of Study 2 were addressed by providing detailed description of the study design, and the procedures followed for data collection and analysis. The collection of both quantitative and qualitative data was used to appropriately address the different questions of the study. Confirmability was addressed by having the analysis and results discussed with the supervisory team. Identified themes for the qualitative data were discussed and revised by the researcher and the supervisory team to agree on the final output. Also, part of the study was peer-reviewed and published (Franqueira et al., 2018).

The limitation was in the convenience sampling approach used. The survey link was sent to individuals whom the researcher had connections with. It could not be sent to every single DF practitioner worldwide. However, results showed a fair variance in the demographics, geographical area, and DF experiences of the participants (see Chapter 6). The sample size for the study was adequate compared to other surveys in the field (see Chapter 6, Section 6.1). That is, given the fact that the study focused on DF practitioners who usually have very busy schedules that might have prevented them from participating in the survey. Other participants whom did not complete the survey stated that their expertise was in fields other than SIEC and cyberstalking and therefore could not provide useful information for the survey. The majority of the respondents were males. The female respondents consisted of only 11.3%, which might have affected the results as females might have had different opinions than males. However, this was expected as both the Law Enforcement and the Digital Forensics fields are highly dominated by male practitioners and male perspectives. Most of the respondents were from Europe (40.4%), which may represent geographical region bias.

Also, there is a possibility that the perceptions and opinions of DF practitioners whom participated in the study were more positive about BA from those who chose not to participate. This might have affected the results providing more positive responses regarding the use and perceived benefits of BA.

3.7 Study 3 (Case study)

The final study proposed a DF investigation process model that incorporated aspects of BA based on input from studies 1 and 2. It aimed to provide a pragmatic, structured, multidisciplinary approach to performing a post mortem examination, analysis, and interpretation of the contents of the digital devices associated with computer-facilitated interpersonal crimes. A case study strategy was adopted to illustrate the investigative importance and utility of the model. Two cases of computer-facilitated interpersonal crimes were selected to illustrate how the model can be used as a DF process for investigating them. In examining each case, the researcher followed the phases and sub-phases of the model developed and described how each of them was conducted in relation to the case. A general discussion was then provided to identify how the application of the model contributed to the investigation of the case. It also compared results of the conducted examination to results from the original case report. The case study strategy was employed to provide a descriptive, in-depth analysis of each case, and provide a clear step by step guide on how to apply the different phases and sub-phases of the model.

3.7.1 Test Environment and Requirements

The study was conducted at the secure lab of the Department of Electronic Evidence – General Department of Forensic Science and Criminology – Dubai Police. For details of the hardware and software used refer to Section 3.5.1.1.

3.7.2 Case Selection and Sample Size

The selection of the sample cases followed the same procedure described in Section 3.5.1.2, utilising convenience sampling (Etikan et al., 2016). Two computer-facilitated interpersonal crime cases obtained from the Dubai Police archive were used: (1) impersonation and defamation on Facebook, (2) employment and money-forwarding scam. The selection of cases was based on the following criteria: (1) offender behaviour which met the definition of interpersonal crimes (i.e., digital crimes involving human interactions between offender(s) and victim(s)), (2) use of a computer as the main offending platform, (3) the availability of bit-wise image files, and (4) the availability of interview scripts with offenders/victims. The cases were crimes committed in Dubai between 2009 and 2013.

The two specific cases were selected as they represented two different types of typical interpersonal digital crimes, and provided a level of complexity (involving at least three types of criminal conduct as described in Chapter 7) without overwhelming the reader with too much detail.

3.7.3 Data Sources

The primary data source for this study was the electronic data (e.g., documents, images, emails, chat logs, Internet cache and history files) stored on the image files acquired of the contents of the seized computer hard-disk drives for each case. Also, for each case, all the related police documents were used to conduct the DF investigation (e.g., background of the offence, interview scripts).

3.7.4 Data Collection

This study followed the phases and sub-phases described in the proposed model (see Chapter 7) to perform a behavioural DF investigation on the selected cases. As such, it collected data that is related to solving each case by identifying the probable offender, identifying offender motivation, understanding the circumstances surrounding the crime, and reconstruction of the crime events. This data was then compared to the results in the original police report. Detailed steps are described in Chapter 7.

3.7.5 Data Analysis

This study followed a behavioural DF investigation model of two real crime cases to illustrate the utility of the model proposed in Chapter 7. It resembled a real DF investigation of computer-facilitated interpersonal crimes. The study did not use any statistical or thematic analysis of the collected data. However, results found by the researcher were compared to the findings in the original police reports. Details are outlined in Chapter 7.

3.7.6 Reliability and Limitations

The credibility, transferability and dependability of Study 3 were addressed by providing detailed description of the steps conducted for each investigated case (see Chapter 7). Confirmability was addressed by having the results discussed with the supervisory team. The use of *real* crime cases in testing the usability and utility of the proposed behavioural DF model also increases the credibility of the findings, as opposed to the use of fictional scenarios performed in earlier studies identified in the literature (e.g., Silde and Angelopoulou, 2014). Performing two case studies on two different variations of computer-facilitated interpersonal crimes addresses transferability of the results.

Confirmability was enhanced, and bias was reduced by the researcher working with a multidisciplinary supervisory team discussing the different stages of performing the DF investigation in each case study and the interpretation of the collected evidence. Investigating each individual case *afresh*, without reviewing the results in the original case documents also

ensured that the findings of the study were not influenced and biased by the results in the original report. The 15 years' experience of the researcher in investigating digital crimes also aided in controlling bias by trying to stay objective through the different stages of investigating the sample cases.

4 TESTING THE UTILITY OF BEHAVIOURAL ANALYSIS IN THE DIGITAL FORENSICS INVESTIGATION OF SEIC CASES

4.1 Introduction

As the literature review demonstrated, the utility of Behavioural Analysis (BA) has gained attention in the field of Digital Forensics (DF) in recent years (Casey et al., 2014, Rogers, 2015, Rogers and Seigfried-Spellar, 2014, Silde and Angelopoulou, 2014, Turvey, 2011). It has been recognised that BA can assist the DF investigator in producing a more justifiable and coherent reconstruction of the crime, in interpreting associated digital evidence, and with the description of investigative findings (Casey et al., 2014, Rogers, 2015, Turvey, 2011). Despite these potential benefits, the literature shows limited use of BA for the DF investigation of computer-facilitated crimes. This study represents a step towards addressing this gap, and fulfilling the first two objectives of the thesis: (1) examining the usability and applicability of BA in the examination, analysis, and interpretation of digital evidence, and (2) examining the ability of BA to contribute to theoretical understanding of the motivational and behavioural dynamics of computer-facilitated interpersonal crimes. It reports on the forensic analysis of 15 cases involving the possession and dissemination of Sexually Exploitative Imagery of Children (SEIC) obtained from the Dubai Police.

The selection of this crime category for the study was for two reasons. First, there is a relatively small body of empirical research on the behaviour and characteristics of online SEIC offenders, with an emerging body of literature examining their demographics and motivations (Babchishin et al., 2015, Henshaw et al., 2015, McGuire and Dowling, 2013, Wolak et al., 2008). Second, the investigation and prosecution of SEIC cases require more than simply locating the abusive files on the suspect's digital device. For example, it is necessary to prove (using the available digital evidence) that the suspect was knowledgeable/aware of the download of SEIC in order for them to be prosecuted (Akdeniz, 2016, Walsh et al., 2013). The use of technology in the commission of SEIC offences, however, raises significant investigative and evidential challenges (e.g., multiple computer users, the increased use of strategies to evade detection, the claim of unintentional download of SEIC) (Balfe et al., 2015, Internet Watch Foundation, 2016, Walsh et al., 2013), and the theoretical and empirical literature on these criminal activities is still in the early stages of development (Houtepen et al., 2014, Taylor, 2001). To date, none of the existing DF research that has incorporated the strategies and principles of BA have been used to empirically investigate SEIC cases.

This chapter reports on the results of the study (for the study design and data analysis refer to Chapter 3). Sections 4.2-4.5 describe the results, while section 4.6 provides a summary of the potential interpretation and investigative utility of the digital evidence in SEIC cases. Section 4.7 discusses the findings, and section 4.8 draws conclusions.

The work presented in this chapter has been published in the proceedings of the 10th International Conference on Availability, Reliability and Security (ARES) (Al Mutawa et al., 2015).

4.2 Location of Potential Sources of Evidence

This section addresses the first set of investigative questions presented in the study design (see Chapter 3 Section 3.5.1). Results indicated that the main source of evidence for this crime category was the computer of the offender. However, in two of the cases, copies of SEIC files were also found on portable hard-disk drives owned by the offenders. It also showed that in cases were the offender owned multiple computers, evidence of SEIC was usually stored on only one of their computers.

In the analysed cases, offenders depended mainly on Peer-to-Peer (P2P) client software for the download and sharing of SEIC. However, in 27% of the cases offenders also used web browsers to search for and download SEIC. In 73% of the cases, evidence of deleted SEIC files and/or evidence of uninstalled P2P client software and directories were found on the offenders' computers.

Offenders used a diverse range of P2P software clients (e.g., shareaza, uTorrent, edonkey, emule, sharestatic, edonkey2000, bittorrent). However, regardless of the type of P2P client software, the most common place to locate evidence is the program files and directories. In most of these programs, a share folder is created where the downloaded files are stored and shared by default unless the user of the program sets it not to do so. In many of the programs (e.g., Shareaza) an 'Incomplete' folder is created where chunks of the files being downloaded are stored and shared until the file is fully downloaded. Another common location to identify evidence is the library files of the P2P client software. These files store records of the downloaded files which includes the location, files size, file names, and a thumbnail of the file. User created files can also reveal valuable evidence as some users change the default download folder of the P2P program to one that they create. Users may change the default download folder for different reasons, for example, to save the downloaded files into a directory/partition other than the Operating System's directory (OS), and to prevent their loss if the OS crashed or was formatted. Other users moved the downloaded SEIC files from the default download folder to a user created folder dedicated for SEIC materials.

Determining the sharing settings of the P2P program is also important in this offence category as it demonstrates the offender's intent to share the files of interest. This was determined either through a review of the registry keys, or by creating a VMware of the offender's computer. A review of the registry keys can also show the search terms the offender entered into the P2P client software, which could establish criminal intent and behaviour (e.g., search terms related to SEIC material in terms of age preferences, gender preferences, and type of sexual activity).

In cases where no evidence was visibly available in the initial examination of the file system structure of the offender's computer, carving the unallocated space (i.e., searching for and extracting files from raw data based on the format characteristics and contents of the files) revealed artefacts, remnants, or complete files that supported the case. These artefacts included evidence that P2P client software had been used, SEIC files had been downloaded, and complete "active" SEIC files.

4.3 Offender Characteristics

This section addresses the second set of investigative questions presented in the study design (see Chapter 3 Section 3.5.1). The main findings of the analysis are shown in Table 4.1 and 4.2. As shown in Table 4.1, offenders did not share a common demographic profile. They ranged from 24 to 46 years of age, and came from a variety of ethnic backgrounds. Far Eastern and South Asian offenders accounted for the highest proportion in this crime category (53%), while Middle Eastern were the least represented (13%). Offenders of Caucasian ethnicity were around (33%) of the total number of the selected cases. All of the offenders were employed at the time

of arrest. However, they varied in occupational status. One offender was a senior executive, three had white-collar jobs, one was a student, and the rest were blue-collar workers. None of the offenders had previous arrests in cases involving the possession and dissemination of SEIC. However, one was previously arrested in an attempt of physically soliciting a minor, while another was arrested for another minor offence. None of the offenders had committed violent offences which had come to the attention of law enforcement. Finally, around two thirds of the arrested offenders (67%) came to the attention of law enforcement through online monitoring, while one third (33%) were arrested after receiving complaints from individuals outside of law enforcement.

Offender Characteristics	**Percentage**
Age range	24 - 46
Caucasian ethnicity	5/15 (33%)
Middle East	2/15 (13%)
Far east and South Asia	8/15 (53%)
Employed at the time of arrest	15/15 (100%)
Professional status	
High professional status	1/15 (7%)
Middle professional status	3/15 (20%)
Low professional status	10/15 (67%)
Student	1/15 (7%)
Came to the attention of law enforcement	
While online monitoring of P2P Networks	10/15 (67%)
Via complaints from individuals outside of law enforcement	5/15 (33%)
Criminal history	
Prior contact offence with a minor	1/15 (7%)
Prior other nonviolent offences	1/15 (7%)
No prior arrests	13/15 (87%)

Table 4.1 Characteristics of SEIC offenders.

4.4 Offending Behaviour

Offenders were mainly viewers, downloaders and sharers of SEIC. None of them produced or used SEIC for financial gain. The SEIC that they possessed were mainly downloaded from the Internet through P2P file sharing networks. Two thirds of the offenders (67%) also used web browsers to search for and download SEIC. For all of the analysed cases, examining the web browsers' cache files, Internet history files, emails, and chat logs did not reveal evidence that the offenders had participated in online offender networks or communities. However, in one case the offender had a previous arrest in an attempt to physically groom a minor. In 87% of the cases, the P2P software clients were set to share the contents of the share folder, which included SEIC files. In terms of the format of the SEIC material, evidence (i.e., downloaded, saved, or viewed SEIC files, as well as folders that contained SEIC materials) showed that offenders were mainly interested in visual files of SEIC, and not in written materials.

Results also indicated that the majority of the offenders were not only interested in SEIC. 80% of the offenders had at least between 40-100 images of other paraphilic materials including bestiality and fetishism. In terms of the volume of SEIC, the majority of offenders (66%) were in possession of an estimated number of images that ranged between 501-5000 files. 20% were in possession of between 101-500 files, while 13% were in possession of over 5000 files. Examining the directories where SEIC were stored showed that most of the offenders (87%) were not concerned with organising and sorting their files. In most of the cases, besides storing SEIC files in the P2P share folder, a few copies of the files were also scattered in different user-created folders. Only two of the offenders (13%) made the effort to sort and categorise their SEIC files.

Assessing the offenders' anti-forensics skills and sophistication in hiding their offending activities indicated that 93% attempted to conceal their possession of SEIC using very basic methods. 73% had simply deleted their SEIC files, and uninstalled the P2P client software. 20% attempted to conceal SEIC files by creating a tree of nested directories with unsuspecting names and storing the files within them. There was no evidence that any of the offenders had used wiping tools to conceal traces of SEIC, used private or anonymous web browsing, or at least used passwords to protect the files. Only one offender showed a level of technical sophistication by using encryption on an entire hard-disk drive.

Offender Behaviour	**Sample Percentage**
Method of obtaining SEIC	
Downloaded through P2P networks	15/15 (100%)
Shared through P2P networks	13/15 (87%)
Downloaded through web browsers	10/15 (67%)
Participated in online communities	0/15 (0%)
Offender Category	
Viewer	5/15 (33%)
Downloader	15/15 (100%)
Sharer	13/15 (87%)
Producer	0/15 (0%)
Trader	0/15 (0%)
Format of SEIC materials	
Video files	15/15 (100%)
Images	15/15 (100%)
Stories	0/15 (0%)
Other paraphilic material	12/15 (80%)
SEIC organised/categorised	2/15 (13%)
Use of countermeasures to avoid detection	
Attempted to hide SEIC files	3/15 (20%)
Deleted SEIC files/programs	11/15 (73%)
Used wiping tools to hide traces of SEIC	0/15 (0%)
Used encryption	1/15 (7%)
Volume of SEIC	
1-100 files	0/15 (0%)
101-500 files	3/15 (20%)
501-1000 files	5/15 (33%)
1001-5000 files	5/15 (33%)
5000+ files	2/15 (13%)

Table 4.2 Offending behaviour in SEIC cases.

4.5 Offender Justifications and Motivations

Thematic analysis of interview scripts with offenders led to the emerging of six explanations/justifications by offenders for committing the SEIC offences: (1) accidental access, (2) another user accessing the subject computer, (3) coping with loneliness/replacement for an absent relationship, (4) substitute for contact offending, (5) encouraged by someone else,

and (6) belief that viewing SEIC does not harm the child victims. Some of these are consistent with the strategies identified by Winder and Gough (2010) that offenders use to justify or defend their behaviour, and to distance themselves from their actions. Table 4.3 shows a number of quotes of offenders extracted from their interrogation scripts.

SEIC Offenders justifications	**Offenders quotes**
Accidental access	▪ *It was by accident.. I search for many kinds of movies you know [through P2P software].. I don't understand English much... I clicked on a file and that's what I got [video of SEIC]..* ▪ *I admit I sometimes look for pornography.. yes.. but not children [SEIC].. it was by mistake [accident].. they just showed up [images of SEIC].. while I was browsing for adult pornography..*
Another user accessing the subject computer/ the computer had a previous owner	▪ *I do not know.. other people used the computer before I did.. one of them might have downloaded them [SEIC files].. definitely.. (subject computer at workplace)* ▪ *My laptop is a second hand.. I bought it from [person's name].. I don't know about these files [SEIC], I didn't download them..*
Coping with loneliness/ replacement for an absent relationship	▪ *I am alone.. I left my family and am here to work.. all by myself.. I do not want to do anything wrong [contact sexual offending, infidelity].* ▪ *I feel lonely.*
Substitute for contact offending	▪ *I only watch videos [adult pornography/SEIC].. It keeps me from doing anything physical [contact sexual offending].* ▪ *I am a lonely man.. you know what I mean.. this [SEIC] helps without the need to go outside.*
Encouraged by someone else	▪ *[person's name] first showed me these [SEIC].. I didn't know about it before.*
Belief that viewing SEIC does not victimise the child victims	▪ *I did not participate in the making of these files [SEIC].. I did not abuse any child.* ▪ *The files [SEIC] were already there [on the Internet].. I only viewed them..* ▪ *I did not create any SEIC files, I did not harm any child, I am only viewing what's already there.*

Table 4.3 SEIC offender justifications and motivations inferred from interview scripts.

It is also worth noting that these interviews were conducted by the police during the course of the investigation. They were not performed for clinical reasons or to understand the motivations underpinning the behaviour of the offender. Also, it was not an interview of self-reported SEIC offenders. As such, it is normal to expected that the offenders will most probably not admit to behaviours that relate them to having sexual interest in viewing SEIC. They will be more likely to try to defend themselves to avoid being convicted and prosecuted.

4.6 Potential Interpretation and Investigative Utility of the Digital Evidence

The interpretive and investigative utility of the digital evidence in SEIC cases identified from examining the sample cases is summarised in Table 4.4. This demonstrates the utility of the combined analysis of the different types of digital evidence in this crime category. It aims to assist in establishing the significance of the processed digital evidence, and help the investigator to form hypotheses about the suspect's actions. This can enable a more detailed reconstruction (i.e., establishing the series of events that surrounded the commission of the offence) of evidence that can inform sentencing and prosecution.

The investigated sample cases did not include any evidence of online communication between offenders and victims, or offenders with other online offenders. Evidence of these activities include chat log files, emails, cached files of web blogs. Also, the sample cases did not include evidence of the user subscribing to websites that provided access to SEIC (e.g., cached web pages showing user subscription, email confirming user subscription). This evidence, however, was added to Table 4.4 to show their benefit and investigative utility in SEIC cases.

Digital Evidence	**Behaviour indicated *(context)***	**Investigative utility**
Registry files: User profiles Password protected		▪ Determines the individuals who had access to the machine. ▪ If only one user profile plus password is protected, it provides a stronger indication that only the owner can access the machine. ▪ Connects other possible suspects to the investigated crime.
Written online communications (e.g., emails, chat logs, text files)	▪ Signature behaviours of the offender (e.g., repeated syntax, spelling, or grammar mistakes, nicknames). ▪ Motivation of the offender (e.g., sexual, financial gain).	▪ Identify signature characteristics of the offender. This can help identify the offender in cases of having multiple users of the computer. ▪ Can reveal the motivation/intentions of the offender. ▪ Identify links/traces to other possible suspects. ▪ Can reveal online communication with offender networks or potential victims.
The location of SEIC files: In user created folders	▪ The user had intentionally downloaded/saved the files on their computer. ▪ The user had interest in the files.	▪ Provides evidence of intentional possession of the SEIC files.
In P2P shared folder	▪ Shows the interests of the user as they searched for and downloaded these	▪ Provides evidence of intentional possession of the SEIC files and/or their dissemination.

	files. ▪ Shows the user is sharing the files (either intentionally or unintentionally).	
Partial files in P2P incomplete folder	▪ The user had searched for and downloaded the SEIC files.	▪ Provides evidence of intentional possession and/or dissemination of the SEIC files.
In web browser cached files, and history files	Depending on the volume of the files, and considering other factors (e.g., search queries, the frequency of visiting the websites): ▪ The user intentionally searched for and viewed SEIC, without the purposeful act of downloading or saving them to their device; or ▪ The user had accidentally viewed these files.	Depending on the volume of the files, and considering other factors (e.g., search queries, number of times the websites have been visited): ▪ Can provide sufficient evidence that the user intentionally sought out SEIC and exercised control over them (by viewing them on their screen). ▪ Can indicate the user had accidentally viewed SEIC (e.g., no search queries of SEIC, no attempts to visit links within the SEIC page such as to enlarge an image of SEIC).
SEIC files links in recently opened files list	▪ The user accessed/viewed the files. ▪ The user had interest in viewing the content of the files.	▪ Provides evidence of intentional possession and use of the SEIC files.
SEIC files attributes in P2P libraries	▪ The user had intentionally downloaded the files at a specific time in the past.	▪ Provides proof that the user downloaded the files. ▪ Provides a timeframe for the downloading of the files, which can be linked to other case-specific evidence (e.g., if the user had committed contact sexual offence in the same timeframe).
SEIC deleted files	Depending on factors such as time stamps, location, and volume of the SEIC files: ▪ The user intentionally possessed the files. ▪ The user had deleted the files to evade detection. ▪ Can indicate the technical skill of the suspect in evading detection; or ▪ May indicate the user's accidental viewing (e.g., a user had a limited number of SEIC cached files, all of which were deleted at once).	▪ Destruction of the files can indicate the user's knowing possession of the files (e.g., a certain number of cached SEIC files existed before but have been systematically deleted over a period of time). ▪ Correlating deletion dates and times to other time stamps can also add to the evidentiary value of the data (e.g., simultaneous deletion of files immediately before seizure of the offender's digital device can indicate their knowledge of being imminently apprehended by the police).
SEIC terms in P2P search queries/web search engines	▪ The user's interest in searching for SEIC. ▪ The search terms used can indicate the content that the offender intended to search	▪ Provides proof that the user actively sought to view SEIC. ▪ Indicates the offender's risk to cross-over to contact offending (e.g., seeking explicit and extreme SEIC is one identified factor

	for (e.g., use of extreme, gross, or violent terms). ▪ Can indicate the gender and age preferences of victims in the images and videos.	for progressing to contact offences) (Johnson, 2015)
Change in the name of the P2P download folder Change in P2P share settings	▪ The user is aware of the existence of the program. ▪ Can indicate the technical skills of the user.	▪ Can be used to determine the technical skills of the user.
The use of anti-forensics to conceal SEIC	▪ The user is aware of the existence of SEIC files. ▪ The user's intention to keep the files and hide if caught by the authorities. ▪ The user is preventing other users from identifying the files on the machines (e.g., family). ▪ The user is aware that possession of the files is wrong/illegal. ▪ Indicates the extent to which the offender is trying to evade detection.	▪ Indicates the technical skill of the offender in evading detection. ▪ Provides evidence of intentional possession and use of the SEIC files, and a strong determination to keep them.
Time stamps of the SEIC files (e.g., created, modified, last accessed)	▪ Variation in a file's time stamps can indicate how the user treated the file (e.g., can indicate whether the user had altered an innocent picture into a SEIC). ▪ Time stamps of the files can suggest how long the offender has been collecting and downloading SEIC.	▪ Provides evidence of intentional possession, and manipulation of the contents of the file. ▪ Assists in constructing a time frame for the length of time the offender has been obtaining these files.
Sorting and categorising SEIC files	▪ Can indicate user motivations associated with the satisfaction of completing a series of images or in sorting the collection in a certain order; or ▪ Having SEIC organised for easier access and later trading with interested individuals.	▪ Provides evidence of intentional possession of the SEIC files, as well as the intention to keep the files for later use.
The presence of files containing other paraphilic materials	Depending on the number of files, and where they are stored: ▪ Can indicate the offender's existing deviant sexual	▪ Sorting through the different types of paraphilic material and their illegality depending on the jurisdiction (e.g., jurisdictions like the UAE prohibits all

	interests.	paraphilic material, while others like the UK do not).
User's subscription to websites that provided access to SEIC	▪ Indicates the extent to which the user is seeking SEIC.	▪ Demonstrates the user's affirmative actions to obtain SEIC. ▪ Can prove intended possession of SEIC.

Table 4.4 A summary of the potential interpretation and investigative utility of the digital evidence in SEIC cases.

A review of the list of digital evidence provided in Table 4.4 show that all of the evidence constitute *context* except for the Registry files. For example, written online communication can reveal the offender's signature behaviour and motivation(s). The location of SEIC files provides indications to whether the offender had intentionally or accidentally downloaded and saved the SEIC files. The frequency of visiting websites that contain SEIC also provides context on whether it was intentional or accidental access of the offending material. Time stamps of the SEIC files provide a timeframe for which the offender have been downloading/accessing the files. Sorting and categorising the SEIC files indicate user motivation (e.g., sorting the files as part of completing a series of images, sorting the files for easy access when trading with other offenders). Corroborating the different types of digital evidence in a SEIC case has a great investigative value as it provides a better understanding of the context surrounding the events of the offence. This can then aid in sentencing and prosecuting.

4.7 Discussion

Exploring the application of BA, including the four stages of BEA within the DF investigation on the SEIC sample cases indicated that not all stages could be utilised in this study. Also, while Turvey (2011) presents the BEA stages in a linear trend, it was not possible to perform it in such a way in practice. Also, the four stages of BEA and the DF stages relating to the examination, analysis and interpretation could not be neatly separated in practice. They intertwined and were performed simultaneously. To simplify the process, the following sections discuss each stage individually providing examples from cases in which it was utilised.

4.7.1 Equivocal Evidence Analysis

As generally described by Turvey (2011), this stage involves a thorough forensics examination and assessment of all the available evidence in a case. It aims to exhaust all assumptions and interpretations of the evidence to identify the limits of the available evidence and what could be achieved using it. This stage needs to be considered within all the steps of the investigative process. To start with, all of the case related documents were carefully studied to understand the

backstory of the case, the involved individual, and the seized devices. Interview scripts with offenders were also analysed to identify inconsistencies in their claims about the offence compared to the identified digital evidence in later stages of the investigation, motivational factors, and justifications for behaviours.

It is essential to perform this stage throughout the DF investigation process as it assists in generating hypotheses in relation to the case, and confirming or refuting them based on facts identified from the digital evidence. For example, in the interview scripts of one of the examined cases, the suspect claimed that he had no idea that the SEIC files existed on the computer and, since the computer had multiple users, someone else might have downloaded the files. Examination of the computer showed, however, that it had three password-protected user profiles. The SEIC files were stored in nested user-created directories that existed under the suspect's user profile. Thus, the identified digital evidence contradicted the claims of the suspect and, assuming that no one else knew his user password, confirmed the suspect's intended possession of the files.

In another case, the suspect claimed accidental access to SEIC files while surfing the Internet. The interpretation of the evidence, however, refuted this claim. Even though the SEIC material was mainly stored in Internet cache folders, artefacts associated with the files contradicted the generated hypothesis of the suspect being an accidental viewer. First, a frequency analysis (Rogers, 2015) of the SEIC files showed that the amount of files was not consistent with the claim of accidental access. Second, timeline analysis (Rogers, 2015) indicated that the website from which the SEIC were viewed has been visited more than once over a certain period of time. Further examination of deleted files also demonstrated that the SEIC were downloaded through a P2P client software and later deleted. As such, with a careful and informed analysis and behavioural interpretation of evidence, the digital investigator can confirm or refute a suspect's claims, assisting greatly in making the appropriate decisions in the legal process.

4.7.2 Victimology

Victimology could not be performed on the sample cases due to the lack of victim-related data such as offender-victim relationship (e.g., written communication, evidence of the suspect being a producer). This, however, could have been useful in other variations of SEIC cases (e.g., offender grooming minors, offender produces SEIC) to understand victim selection for the production of SEIC. This can subsequently help to identify victims and improve safeguarding of minors, as well as offender risk assessment. For example, chat logs could reveal that a groomer was attracted to a specific victim due to them being accessible (e.g., living nearby), being easily controlled by the offender, or being physically or sexually attractive to the offender (e.g., from pictures or interactions). Offending behaviour can also be explored by examining the techniques

the offender employed to entice the victim and groom them for sexual exploitation. This includes the use of a false persona, expressing affection, attention, or concern. These strategies can be used to build a connection with a minor and incite them into sexual activity. Analysis of victimology can also show how a producer influenced and encouraged the victim to self-produce an illegal image using a webcam. Once the offender receives the image, this can be used to coerce the victim into producing more images. As such, this can assist the investigator in identifying the circumstances of the offence. This information can then assist in monitoring these activities online and in sting operations.

Even though the content of SEIC imagery is not routinely examined in the UAE, such examinations can assist investigation and prosecution. For example, identifying the level of severity of the contents can determine different levels of sentencing in the UK (Antoniou and Akrivos, 2017). SEIC materials of more severe and explicit sexual activity, alongside other factors (e.g., large collections of SEIC, contact with like-minded individuals, access to children), can also be indicative of having a higher risk of contact offences (Johnson, 2015). Examining images can also lead to the identification of victims. In addition, it can be used to determine the prevalence of SEIC by identifying the quantity of new imagery being circulated online. This can subsequently aid in combating this crime by identifying trends in SEIC imagery, techniques used in the offending, and strategies to better safeguard children.

4.7.3 Crime Scene Characteristics

In the SEIC sample cases, the digital devices of the suspects constituted the virtual crime scene of the case. It is the crime scene that the DF investigator mainly examines to search for incriminating files, meta-data, or artefacts associated with the case at hand. Other characteristics identified by analysing the crime scene can provide great assistance in confirming or refuting case related hypotheses.

For example, the location of SEIC files can indicate offender knowledge/awareness of the material being on their devices. Some offenders may claim accidental viewing of SEIC while surfing the Internet (Winder and Gough, 2010). However, digital evidence can contradict this claim if SEIC is found to be saved in user created folders. Sorting and categorising the files can further indicate intentional offender behaviour, as well as commitment to their interests through spending time and making an effort to classify the files in a particular manner. This can aid in designing offender interview strategies to gain more insight into the reasons why the offender categorised their SEIC collection. It raises the question of whether the offender sorted the files based on personal and private interests, or whether they were in the initial stages of preparing the files for sharing, distribution, or trading, which prompts a more serious offence. Deliberate attempts to hide SEIC also reflect offender awareness of the existence of these files and their

determination to retain them. It further indicates that they are aware of the legal status of the activities and files, and the potential for detection and prosecution. Evidence of SEIC related queries in P2P client software and web browser search engines also reflect offender interests and intention in finding, viewing, or downloading these files. Combined with complete or partial SEIC files in the P2P's client folders, this supports the hypothesis of the suspect intentionally searching for and downloading the contraband material.

In cases where the offender is a producer of SEIC, their smartphone can be used to produce this material. For example, examining the meta-data of a SEIC image on a suspect's computer and finding that it matches the meta-data of images taken by the smartphone of the suspect can give an indication that the image was actually produced by the offender.

4.7.4 Offender Characteristics

The study results suggest that it is not possible to construct a single profile for SEIC offenders, as this does not reflect the dynamic nature of individuals and their behaviours as reflected in the basic principles of BEA (see Chapter 2). However, most of the identified offender characteristics and behaviours was consistent with prior inductive studies on offenders in the same crime category.

The demographic characteristics of offenders presented in Table 4.1 showed that they are not a homogenous group in this respect, a finding well-supported in other work (Galbreath et al., 2002, Seigfried-Spellar, 2014, Seto and Eke, 2005). Aside from being exclusively male, their age ranged from 24-46, they were of different ethnicities, and were varied in terms of professional status. Unlike findings from other studies (Seigfried-Spellar, 2014, Shelton et al., 2016, Webb et al., 2007), over half of the offenders (53%) were of Far East and South Asian ethnicities. Still, a significant percentage (33%) was of Caucasian ethnicity. This can be explained by the demographics of the country in which the study took place (i.e., the UAE). Given that around 85% of the population of the UAE are expatriates with approximately 60% being from Asia (index mundi, 2017), this result appeared to be reasonable.

Consistent with previous studies (Shelton et al., 2016, Webb et al., 2007, Wolak et al., 2003), the majority of offenders (87%) did not have any known record of previous offences. A small percentage of the sample (14%) (n=2) had a prior offence with a minor, and a non-violent offence. Despite this, it is likely that some of the SEIC offenders had previous undetected offences, as studies indicate that some offenders disclose unreported crimes during treatment (Galbreath, Berlin, & Sawyer, 2002; Webb et al., 2007). All of the offender were employed in different occupations (with 7% being a student) at the time of the offence, which is close to the

findings of Shelton et al. (2016) which found that only 3% of offenders were unemployed and 3% were students.

The preceding stages were also used to identify offending behaviours within each case as presented in Table 4.2. Mapping results onto the SEIC offender typology designed by Krone (2004) showed that all of the offenders in the study sample appeared to fit within the non-secure collector category (see Chapter 2). They mainly used P2P networks to download (100%) and share (87%) SEIC, with a few (20%) applying very basic security measures to hide the material. Offenders also exhibited behaviours that were consistent with that of a browser as well as a trawler. In 33% of the cases, timeline analysis of the SEIC files showed that a number of the files that were viewed through Internet web browsers had older timestamps than those downloaded through P2P applications. This indicated that the offender might have initially viewed SEIC through a web browser (either accidentally or intentionally) before using P2P applications to seek more of the material. This suggests that the offender might have started as a browser or a trawler, and then progressed to being a non-secure collector, posing the question of whether their behaviour would escalate further to a higher level of offending. It is important to question whether the SEIC offender is involved in other levels of offending. Behavioural interpretation of the digital evidence can provide predictive indications about the level of involvement which can subsequently aid in the investigation of such cases.

The offenders in the sample cases did not exhibit behaviours indicative of producing and/or trading SEIC. Digital evidence associated with producing SEIC, for example, can include SEIC imagery produced through a webcam along with chat logs containing indicative conversation between the offender and the victim depicted in the SEIC material. As for trading SEIC, evidence can include emails or chat conversations referring to the exchanging of material. Evidence of sending or receiving the subject SEIC files can also support the offence of trading SEIC. Payments made to specific SEIC services (e.g., by credit card) and login credentials also adds to evidence of this SEIC offending category.

The results also indicated that the motivation of the majority of the sampled SEIC offenders appeared to be to obtain sexual gratification from viewing SEIC. None of the offenders were involved in financial gain through SEIC. Further, the majority of offenders (80%) had a variety of indiscriminate deviant sexual interests that included bestiality and fetishism. None of the offenders had any online communications with like-minded online individuals, or had attempted to groom minors online. One offender, however, might have attempted to progress to contact sexual offence with a minor by making him watch a SEIC video that was stored on his mobile phone.

The study also explored the way in which offenders justify their behaviour. Six key themes emerged from the data: (1) accidental access, (2) another user accessing the subject computer, (3) coping with loneliness/replacement for an absent relationship, (4) substitute for contact offending, (5) encouraged by someone else, and (6) belief that viewing SEIC does not harm the child victims. However, it is important to note that offenders may have not provided honest accounts of their offending behaviour. As the interviews were a result of police interrogations, offenders may have sought to distort or lie about aspects of their stories in order to avoid conviction. As previously described, accidental access has been refuted in a case when behavioural analysis of the digital evidence was compared to the claims made by the offender. In two of the cases where offenders claimed that the SEIC belonged to another individual, analysis of the digital evidence contradicted their statements. Timeline analysis of the SEIC files showed consistency with time windows where the offender was using the computer that contained the material. This demonstrates that the DF investigator must always consider statements made by offenders and victims while examining and analysing the digital evidence, and compare the identified behaviour in order to support or refute their claims.

An interesting finding was that three of the offenders who justified their behaviour as the results of coping with loneliness or as a replacement for an absent relationship also believed that viewing SEIC does not harm child victims. Their lack of victim empathy, along with poor problem solving in relation to their loneliness in addition to other factors that might be present (e.g., sexual preference for children, time spent to collect SEIC, level of SEIC severity) can be indicators for the likelihood of progressing to contact offences (Johnson, 2015). This must be considered by the DF investigator to assess the risk the offender poses in terms of escalation of their offending behaviour.

4.7.5 Contribution to the Digital Forensics Investigation of SEIC

The current study explored the ways in which BA, including stages of its subset BEA, can be applied to the DF investigation process in SEIC cases, and what it contributes to the investigation. After exploring how BA can be integrated within the DF investigation process of the sample cases, results were compared to those of the original case reports. The original reports, however, provided limited information with regard to the structure of the DF process performed for the examination, analysis, and interpretation of the digital evidence within each sample case. Depending on what was requested in each case, the "results" section of the original report provided similar technical findings with regard to the identified SEIC files, the means by which they were obtained, their locations, their quantity, and their timestamps. They also provided information on other paraphilic material in the possession of the offender. The reports did not provide any indication with regard to identified offender motivations, SEIC preferences

and collection organisation, nor did it compare findings from digital evidence to claims made in offender statements.

The original reports mainly focused on stating the technical facts found during the examination and analysis of the digital evidence, and this can be sufficient in sentencing and prosecuting the SEIC offences in this sample of cases. Corroborating the technical findings with offender statements could also be the work of a party other than the DF investigator. However, providing greater consideration to the behavioural and motivational factors in a SEIC crime (as shown in the preceding sections) can provide important insights into offending behaviour in this crime category. As previously shown, it is important to gain greater understanding of SEIC offenders in the interest of safeguarding minors, prevention, and detection. It is also essential to recognise when SEIC material is part of an individual's sexually exploitative behaviour. Uncovering digital evidence can be an initial step in a multi-layered investigation into a more severe crime (e.g., child sexual abuse).

An identified limitation in relation to the findings of the study was that all of the offenders in the SEIC sample cases appeared to fall within a single offender typology (i.e., unsecure-collector) as described by Krone (2004) (see Chapter 2). This offending behaviour seemed to be the trend in the cases investigated by the Dubai police at the time the offences took place. This, however, limited the researcher's ability to empirically study other types of digital evidence related to SEIC offending behaviours that map to the other offender categories identified by Krone (2004).

4.8 Summary

This study aimed to address two objectives of the programme of research: (1) examining the ability of BA to assist in the examination, analysis, and interpretation of digital evidence, and (2) examining the ability of BA to contribute to theoretical understanding of the motivational and behavioural dynamics of computer-facilitated interpersonal crimes. Previous studies depended on inductive approaches to understand the offending behaviour of criminals arrested in SEIC offences. This study, however, followed an abductive approach by examining each case separately, applying digital forensic analysis and BA to understand the behavioural dynamics of offenders in this crime category, and performing statistical analysis to compare results to previous research. To address the two main objectives of the study, a number of sub questions (see Chapter 3) were identified and explored throughout the stages of the study.

The preliminary findings showed that utilising BA in computer-facilitated interpersonal crimes can benefit the investigation process in a number of ways. First, it provides a structured approach to direct investigators to potential sources of digital evidence on the examined

devices. It also provides insight into specific offender characteristics and behaviours that can assist risk assessment. However, the main outcome of the study was establishing a method for interpreting digital evidence to achieve better explanation of the events of the crime that will aid in prosecuting SEIC cases. Table 4.4 can assist in establishing the significance of the processed digital evidence, and help the investigator to form hypotheses about the suspect's actions. This can enable a more detailed reconstruction of evidence that can inform sentencing and prosecution. Also, this study focused on a specific category of computer-facilitated interpersonal crime and was designed to enable it to be utilised in investigating individual cases and understanding the dynamics and behaviour of individual offenders. The interpretation table (Table 4.4) can also be utilised by prosecutors to establish a bridge between the behavioural and technical aspects of digital evidence. This can enable them to better understand the utility of specific digital evidence in supporting the prosecution of SEIC crimes.

Exploring the ways in which BA can be integrated within the DF investigation process of the SEIC sample cases provided an insight into the extent and limits to which BA can be utilised. The interpretation table provides detailed insight into what to look for in an investigation. This will be further explored in the next chapter and the combined results will aid in identifying the necessary structure to design a DF investigation model that will aid DF investigators to complete each step of the examination, analysis, and interpretation of digital evidence to achieve reliable results.

5 TESTING THE UTILITY OF BEHAVIOURAL ANALYSIS IN THE DIGITAL FORENSICS INVESTIGATION OF CYBERSTALKING CASES

5.1 Introduction

The review of literature demonstrated that Behavioural Analysis (BA) is, in theory, useful in developing an understanding of the offender, the victim, the crime scene, and the dynamics of the crime (Casey et al., 2014, Rogers, 2015, Turvey, 2011). It can aid with the interpretation of the evidence extracted during the Digital Forensics (DF) techniques and assist investigators with reconstruction of the crime (Casey et al., 2014, Rogers, 2015, Turvey, 2011). Yet, this area of research is under-researched and lacks empirical testing, especially in relation to crimes facilitated by technology. The previous chapter explored the application and the utility of BA to the DF investigation of cases of the possession and dissemination of Sexually Exploitative Imagery of Children (SEIC). This chapter continues to address the first two objectives of the thesis: (1) examining the usability and applicability of BA in the examination, analysis, and interpretation of digital evidence, and (2) examining the ability of BA to contribute to theoretical understanding of the motivational and behavioural dynamics of computer-facilitated interpersonal crimes. It follows on from the study conducted in Chapter 4 by exploring the application and the utility of BA on a second category of computer-facilitated interpersonal

crime: cyberstalking. It reports on the forensic analysis of 20 cases of cyberstalking obtained from the Dubai Police.

The crime category of cyberstalking was selected for this study for a number of reasons. The use of advanced technologies to commit cyberstalking raises significant investigative and evidential challenges (Brown, 2015, Fusco, 2014). In this crime category, digital evidence and artefacts do not reside on a single electronic medium, but are scattered across several electronic mediums (e.g., offender/victim devices and within the online environment) (Aggarwal et al., 2005, Bryce et al., 2016). Also, despite the serious harm that it can cause (e.g., inflicting emotional distress, physical harm, murder, suicide), it remains an under-prosecuted offence (Vasiu and Vasiu, 2016). The theoretical and empirical literature on the behaviour and characteristics of cyberstalkers is limited. Nevertheless, behaviour associated with this offence category generates specific forms of evidence which can be extracted from digital devices during the DF investigative process. This evidence can then be analysed using BA in order to build a specific profile of offenders to determine the motivations associated with their behaviour, their relationship with the victim(s), risk of progression to physical stalking, and the interpretation of digital evidence.

The chapter is organised as follows. Sections 5.2-5.6 reports on the results, and section 5.7 summarises of the potential interpretation and investigative utility of digital evidence in cyberstalking cases. Section 5.8 discusses of the results, and finally, section 5.9 provides a summary of the chapter. The work done in this chapter has been published in the proceedings of the Third Annual DFRWS 2016 Europe (Al Mutawa et al., 2016).

5.2 Location of Potential Sources of Evidence

Digital evidence associated with this crime category was found on both the offender's and the victim's computers. However, in many of the cases the DF investigation started by receiving and examining the victim's computer(s), leading to initial evidence being extracted from their computer(s). In case where an offender or a suspect was apprehended, their computer(s) were also seized for examination.

In the analysed cases, offenders mainly used emails, social networks, dating web sites, and forums to harass their victims. As such, relevant digital evidence was usually found and extracted from files and folders that store data and artefacts related to the user's online activities, such as Internet history files, cache files, and data files related to email clients (e.g., MS Outlook PST files). These files could constitute evidence of email messages sent to the victim, evidence of the offender accessing the online social networking profile of the victim, uploading the victim's picture online, and posting defaming messages.

The Unallocated Clusters of the hard-disks also provided useful evidence. For example, it contained partial or full files of the harassing emails, and partial files of the victim's pictures related to the offence.

5.3 Victim and Offender Characteristics

This part of the analysis aimed to identify the characteristics of offenders and victims. The results of the analysis are presented in Table 5.1. The age of the victims and offenders varied. Victims ranged from 23 to 48 years of age, while offenders ranged from 21 to 63 years of age. The majority of the victims were females (75%), consistent with other research findings (Stephenson and Walter, 2011) yet, there were also males that were victims of cyberstalking (25%). In terms of ethnicity, a lower percentage of East Asians and South Asians (25%) experienced cyberstalking compared to Middle Easterners (45%) and Caucasians (30%). The majority of the offenders and victims were employed at the time that the offence occurred (80% for both), though their professional status varied: 10% of victims had a high professional status, and the majority (60%) were of a middle professional status. None of the offenders were of high professional status, 70% were of middle professional status, and 20% were of low professional status. Only two of the offenders were known to have previous convictions for assaulting others.

Characteristics	Victims	Offenders
Age range	23 - 48	21 – 63
21 - 30	8/20 (40%)	4/20 (20%)
31 - 40	6/20 (30%)	7/20 (35%)
41+	6/20 (30%)	9/20 (45%)
Gender		
Female	15/20 (75%)	4/20 (20%)
Male	5/20 (25%)	16/20 (80%)
Ethnicity		
Caucasian ethnicity	6/20 (30%)	7/20 (35%)
Middle East	9/20 (45%)	8/20 (40%)
Far east and South Asia	5/20 (25%)	5/20 (25%)
Professional status		
High professional status	2/20 (10%)	0/20 (0%)
Middle professional status	12/20 (60%)	14/20 (70%)
Low professional status	3/20 (15%)	4/20 (20%)
Student	1/20 (5%)	0/20 (0%)
Unemployed	2/20 (10%)	2/20 (10%)

Table 5.1 Characteristics of cyberstalking victims and offenders.

5.4 Victim/Offender Prior Relationship

Table 5.2 describes the gender and prior relationship between offenders and victims. Unlike results from other studies (e.g., McFarlane and Bocij, 2003), all of the victims and offenders had a prior relationship. None of them were total strangers. 35% had a previous intimate relationship, and 40% were work colleagues. 10% were acquainted, and 10% met online. Further, the majority of the cyberstalkers were males (80%). In most of the cases (60%) females were stalked by males, and in 20% of the cases males stalked males. However, the data also showed that females could be cyberstalking offenders. In one case a female cyberstalked a male, and in three other cases females stalked other females.

Relationship	Percentage
Ex-intimates	7/20 (35%)
Acquaintances	2/20 (10%)
Work Colleagues	8/20 (40%)
Met online	2/20 (10%)
Total strangers	0/20 (0%)
Unknown	1/20 (5%)
Gender cyberstalking	
Male-female stalking	12/20 (60%)
Female-male stalking	1/20 (5%)
Female-female stalking	3/20 (15%)
Male-male stalking	4/20 (20%)

Table 5.2 Gender cyberstalking and offender/victim relationship.

5.5 Offending Behaviour

The analysed data showed that emails were the most prevalent means of offending in cyberstalking incidents, as shown in Table 5.3. In more than half of the analysed cases (55%) the cyberstalkers depended on emails to initiate contact with their victims. In 15% of the cases, the offenders communicated with their victims via their personal email accounts. In 25% of the cases, the communication was through the victims' workplace email accounts, and in 15% of the cases the offenders had access to their victims' email accounts and used this to impersonate them. The next most frequent method of offending was through social networking websites (25%); mainly Facebook and Twitter. Cyberstalkers used these websites to post embarrassing, hateful, or threatening comments about their victims. Dating websites (15%) were mainly used to impersonate the victims, to post false comments regarding the sexual fantasies or desires of

the victims, and encourage visitors to contact them. From all the analysed cases, only two victims had also experienced offline stalking from their cyberstalker. Also, in one case the cyberstalker used surveillance on his victim; he had installed a Global Positioning System (GPS) tracker on the victim's car.

In the majority of the analysed cases (60%), the cyberstalking offence lasted between three weeks and six months. It lasted between 7 months to a year in 20% of the cases, and lasted for two years in one case (15%).

Offending behaviour	Percentage
Cyberstalking duration	
6 months or less	12/20 (60%)
7 month – 1 year	4/20 (20%)
2 years	1/20 (5%)
Unknown	3/20 (15%)
Means of offending	
Emails	11/20 (55%)
Social networking web sites	5/20 (25%)
Personal chat services	0/20 (0%)
Forums and bulletin boards	1/20 (5%)
Dating web sites	3/20 (15%)

Table 5.3 Means and length of cyberstalking

Thematic analysis of the offender's actions indicated by the digital evidence identified seven offending behaviour themes in the sample cases: (1) false accusations of victims/defamation, (2) impersonation, (3) obsession, (4) blackmailing/threatening, (5) collecting information about the victim/tracing the victim, (6) violation of privacy, and (7) extortion. Table 5.4 describes offender actions inferred from the digital evidence as related to each identified theme.

Offending behaviour	Cyberstalker offending behaviour inferred from digital evidence
False accusation of victim/defamation	▪ Posting obscene/morphed images and/or false statements about the victim on social networking sites. ▪ Sending obscene/morphed images and/or false statements about the victim through email to friends/family/work colleagues.
Impersonation	▪ Creating fake social networking accounts in the name of the victim and posting images and personal information of the victim on them. ▪ Sending offensive emails to work colleagues from the victim's email account.
Obsession	▪ Sending emails repeatedly proclaiming love, and showing obsession with the victim. ▪ Sending emails repeatedly mentioning memories of their past relationship. ▪ Sending excessively needy and demanding emails. ▪ Sending intimate/pornographic images.
Blackmailing/threatening	▪ Sending persistent emails that contain threatening phrases. ▪ Posting offensive or threatening messages on the victim's social networking profile.
Collecting information about the victim/tracing the victim	▪ Remotely accessing the victim's computer. ▪ Gathering information about the victim. ▪ Monitoring the victim's online activities through their social networking profile.
Violation of privacy	▪ Publishing or transmitting images of private body parts of the victim without their consent.
Extortion	▪ Threatening to publish/forward victim's intimate/sexually explicit images/information unless being paid a specific amount of money.

Table 5.4 Offending behaviour inferred from the digital evidence.

5.6 Offender Motivations

Thematic analysis of the offender/victim communications led to the identification of four offender motivations: (1) rejected partner seeking revenge, (2) rejected partner trying to reconcile, (3) revenge for actual or perceived injustices, and (4) monetary gain. Table 5.5 illustrates a number of quotes of offenders extracted from the digital evidence found in the analysed cases. Note that the researcher obscured profanity in these quotes.

Cyberstalker motivation	Cyberstalker quotes from digital evidence
Rejected partner seeking revenge	▪ *Ok baby, it's up to you, don't answer me, I opened a facebook account and posted your disgraceful pictures. You are wicked and I don't care what will happen to you.* ▪ *[A$$hole] just want to tell you that I am uploading your sex videos on youtube, have a nice day, I love you baby.* ▪ *Bad girl you are not answering me or are you busy [f@#king] a man on web cam.*
Rejected partner trying to reconcile	▪ *Honey why don't you answer my emails, hope you are fine.* ▪ *Honey I changed my email because so many ladies are disturbing me I don't want to lose you.* ▪ *You are not the baby I used to know, any problem just email me, I love you.* ▪ *My princess, please come online. Miss you so much and I cannot stop loving you.*
Revenge for actual or perceived injustices	▪ *You will regret what you did for the rest of your life!* ▪ *Wherever you are… I will come and get you.* ▪ *[Name of executive of a company] is dishonest, unprofessional and a cheater.* ▪ *You promised to help and now you are no longer answering me, fine, if I lose the contract, I will sell your naked video tape. Where you were [profane description of video content].* ▪ *Dear [victim's name] I ask in every prayer that you and your manager get CANCER because you have stolen Dhs 2,050 from me. I will not stay quiet about this!*
Monetary gain	▪ *Stupid [b@#ch] raise half of that money for me before the 5th of this month or else your little dirty secrets will go viral! You will be famous!* ▪ *I will post your videos [performing sexual acts]on youtube, facebook, and twitter. If you can pay 40,000 Dirhams I will send the videos to you now.*

Table 5.5 Cyberstalking motivation inferred from the digital evidence.

5.7 Potential Interpretation and Investigative Utility of Digital Evidence

The interpretive and investigative utility of the digital evidence identified from examining the sample cyberstalking cases is summarised in Table 5.6. This demonstrates the utility of the combined analysis of the different types of digital evidence in this crime category. It aims to assist in establishing the significance of the processed digital evidence, and help the investigator to form hypotheses about the events surrounding the offence. This can enable a more detailed reconstruction of evidence that can inform sentencing and prosecution.

Digital Evidence	**Behaviour indicated *(context)***	**Investigative utility**
Registry files: Hacking software/spyware	Victim: ▪ Indicates the victim's limited knowledge of computer literacy (e.g., the victim demonstrates little knowledge of protecting their computer from malicious software by not installing an anti-virus software). This can be one contributing factor to their victimisation. Offender: ▪ Indicates offender intention to cyberstalk the victim (e.g., by monitoring their online activities). ▪ Indicates the level of computer literacy of the offender.	Victim's computer: ▪ Indicates whether the victim's machine was compromised and could be remotely accessed by the offender. ▪ Can be checked against the offender's machine to establish links and reconstructions of the crime (e.g., identify whether the offender used the client of the same software to remotely access/monitor the victim's computer). Offender's computer: ▪ Indicates use of hacking/spying software or any other crime-related software used by the offender in their cyberstalking.
Offender/victim written online communications (e.g., emails, chat logs, text files)	▪ Indicates the victim/offender relationship. ▪ Signature behaviours of the offender (e.g., repeated syntax, spelling, or grammar mistakes, nicknames). ▪ Offender motivations (e.g., sexual, hatred).	▪ Indicated victim/offender relationship can be cross-examined against their claims (e.g., claim of not having prior relationship). ▪ Adds to understanding the context of the crime. ▪ Identify signature characteristics of the offender. This can help identify the most probable offender in cases involving multiple suspects. ▪ Can reveal the motivation/intentions of the offender. ▪ Identify links/traces to other possible victims/suspects.
User files and folders. File links in recently opened files list	▪ Indicates victim's interests and lifestyle. ▪ Indicates offender's interests and motivations to commit the offence.	▪ Includes evidence supporting the cyberstalking crime. For example, files of scandalous morphed images of the victim, plus the original picture of the victim, and evidence of using a specific software to create those images.
Web browser cached files, and history files	▪ Indicates victim's online activities, interests, and behaviour (e.g., from search terms, regularly visited social networks) that could potentially expose them to risk of cyberstalking. ▪ Indicates offender's online	▪ Provides a timeline for the online activities of both the offender and victim that can aid in reconstruction of the crime. ▪ Can include other evidences such as web-based chat logs, emails, uploaded images, etc.

	activities, interests, and motivations for engaging in the behaviour.	
Deleted files	On the offender's machine: Examining the contents of the files alongside factors (e.g., type, time stamps, and location of files) can: ▪ Indicate the offender's specific interest in the victim. ▪ Indicate that the offender had deleted the files to evade detection. ▪ Indicate the technical skill of the offender in evading detection.	▪ Destruction of the files can indicate that the offender intended causing harm/distress to the victim. ▪ Depending on the contents of the deleted files, it can further inform the investigation. (e.g., pictures and/or written communications indicating offender/victim prior intimate relationship).
The use of anti-forensics to conceal cyberstalking files/activities	▪ Indicates offender's awareness of the wrong/illegal status of their activities. ▪ Indicates the extent to which the offender attempts to evade detection or conceal evidence if suspected by the victim and reported to authorities. ▪ Indicates the offender's level of technical skills.	▪ Indicates the technical skill of the offender in evading detection. ▪ Provides evidence of the offender's determination to engage in cyberstalking and taking measures to hide their illegal activities.
Time stamps of the evidence files (e.g., created, modified, last accessed)	▪ Variation in a file's time stamps can indicate how the offender treated the file (e.g., can indicate whether the offender had altered an innocent picture of a victim into an obscene image). ▪ Time stamps of the files can suggest how long the offender has been in possession of the files and how long they had been planning to cyberstalk their victims.	▪ Provides evidence of intentional possession, and manipulation of the contents of the file (e.g., victim's pictures). ▪ Assists in constructing a timeframe for the length of time the offender has been obtaining these files and their plans for cyberstalking the victims.
Sorting and categorising victim's files	▪ Indicates offender's organisation, methodological planning and perpetration of cyberstalking (e.g., the offender organises victim files into separate folders with each bearing each of the victim's names).	▪ Provides evidence of other potential victims that the offender intends to, or has already been, cyberstalking.
The presence of files containing paraphilic materials	Depending on the type of the cyberstalking, the number of the paraphilic files, and where they are stored: ▪ Can indicate the offender's existing deviant sexual interests.	▪ Can add to the profile of the offender in determining their motivations for cyberstalking.

Table 5.6 Potential interpretation and investigative utility of digital evidence in cyberstalking cases.

5.8 Discussion

This section discusses the findings from exploring the application of the four stages of BEA (a subset of BA) within the DF investigation of the cyberstalking sample cases. Unlike the findings from the study in Chapter 4, it was possible to utilise all of the BEA stages on this case sample. However, as it was the case with the study in Chapter 4, setting distinguishable lines between the steps of performing the different stages of BEA within the DF process of examining, analysing, and interpreting the digital evidence was not possible. The process was dynamic and stages of BEA intertwined and were performed simultaneously. The following section discusses each stage individually, providing examples from the cases in which it was utilised.

5.8.1 Equivocal Evidence Analysis

As in the previous chapter, this stage was considered throughout all the steps of the investigation process. Whenever evidence files and artefacts were found (e.g., communication logs, emails, pictures of victims), the researcher tried to consider all the different assumptions and interpretations of the files. For example, timestamps and contents of offender communications were corroborated with the victim and/or the offender statements to identify inconsistencies, false victimisation, or hidden motives. Having the victim-related files stored alongside a number of folders that contained information and personal files (e.g., images) of other individuals indicated that the victim might not be the only individual being targeted by the offender. Storing files of adult pornographic material, paraphilic material, or self-produced obscene imagery, and forwarding such files to the victim, might indicate the offender's existing deviant sexual interests.

5.8.2 Victimology

This stage involves understanding the interests and online activities of the victim that might have placed them at risk, or that might have appealed to the offender (Casey et al., 2014, Turvey, 2011). For each case, the researcher performed victimological inquiries to gather sufficient information about the victim to recreate the context to the incident and provide a starting point for the investigation. This information was gathered from the case documents (e.g., victim interview script, background story to the offence), and through the examination of the computers seized in each case. The queries answered in this stage of the analysis included: (1) the victim's daily online routine and habits, (2) online interests and most visited websites,

(3) list of friends/co-workers, (4) previous relationship with the offender, (5) whether the victim suspected someone.

Analysis of the associated interviews showed that most of the victims appeared to have prior offline knowledge of the offender ranging from being ex-intimates, work colleagues, and acquaintances (see Table 5.2). In two of the cases, however, victims had met offenders online through a dating website, and through a social networking website. In the first case, examining files that reflected the victim's online activities (e.g., Internet history files, cache files) showed that the victim frequented the dating website from which she claimed to have met the offender. The victim also had a social networking profile in which she published her personal details including her name, age, location, work, hobbies, and pictures. Examination of the evidence also showed that the victim was the one to initiate contact with male individuals in a number of instances, however, with the case of the offender the one who initiated the contact could not be established from the digital evidence. The social networking chat records that were found demonstrated what appeared to be a romantic relationship that was later ended by the victim (based on the timeline of the exchanged messages). This was what appeared to motivate the offender to cyberstalk the victim. He first tried to restore their relationship (as reflected from his written communications), and when this failed he escalated to expressing rage and threatening the victim.

The previous case demonstrates a number of victim activities that might have increased her risk to being victimised. These included publishing her personal information, and initiating contact with strangers. Ending the relation with the offender might have also triggered his offending behaviour as being rejected in a relationship has been identified in the literature as one motivating factor for cyberstalking (Lowry et al., 2013, McFarlane and Bocij, 2003). However, the offender might also have multiple motivations, highlighting that the DF investigator must keep an open mind to other interpretations.

5.8.3 Crime Scene Characteristics

As with other digital crimes, the physical crime scene is usually absent in cyberstalking crimes, and as such the computer is considered to be the primary crime scene (virtual crime scene). The analysed cyberstalking cases indicated that, similar to offline crime, the offender exhibits and leaves indications of certain behaviours in the virtual environment that can be inferred from the digital evidence (Casey, 2011, Turvey, 2011). Interpretation of the digital evidence extracted from the virtual crime scene can provide assistance to confirm or refute case related hypotheses throughout the investigation. Table 5.6 provides examples of potential interpretations and the investigative utility of the different types of digital evidence that can be found when investigating these cases.

The crime scene was examined for distinguishing features and choices that the offender had made. This included the means by which the offender communicated with the victim, the language used in written communication, and the methods used to harass the victim. This enables the investigator to understand the choices the offender made and the needs they fulfilled by their offending behaviour, and this can help narrow down the suspect pool in cases of unknown offenders (Casey et al., 2014). For example, expressing knowledge of the victim's specific personal details can indicate the offender is someone who had been close to the victim (e.g., ex-intimate), while referring to a work-related issue can indicate the offender being a work colleague or a disgruntled employee. Taking the time and effort to use specific photo editing programs to fabricate an original picture of the victim into an obscene image can indicate the offender's determination to harass the victim. The combined evidence of emails threating to publish obscene pictures of the victim, alongside the morphed images of the victim on the offender's computer, plus evidence of the images being uploaded through the offender's computer, with timeline analysis provides a chronological and a clear understanding of the events of the crime.

The choices of words that the offender used in their written communications with the victim can also indicate their motivation (Table 5.5). For example, some offenders appeared to be trying to re-establish a relationship with the victim:

> *You are not the baby I used to know, any problem just email me, I love you.*
>
> *My princess, please come online. Miss you so much and I cannot stop loving you.*

While others used phrases that indicated anger and revenge for actual or perceived injustices:

> *[Name of executive of a company] is dishonest, unprofessional and a cheater.*
>
> *You promised to help and now you are no longer answering me, fine, if I lose the contract, I will sell your naked video tape. Where you were [profane description of video content].*

Considering the behavioural and motivational factors of offenders as inferred from the available digital evidence can further inform the investigation. In serious cases, this can contribute towards an assessment of the risk that an offender is likely to physically harm their victims or themselves. This can assist investigators to develop an effective strategy to prevent harm to the involved parties. These benefits combine to enable investigators to build a clear case and to reduce mistakes, wasted effort, and the misinterpretation of digital evidence. For example, overlooking exculpatory digital evidence can lead to the prosecution of the wrong individual (Casey et al., 2014). Likewise, misinterpretation of incriminating digital evidence can prevent

proving a case beyond a reasonable doubt. Having a more detailed understanding of offending behaviour can also help with the identification of relevant evidence and its correct interpretation. It also provides context, connections and investigative directions (Turvey, 2011).

5.8.4 Offender Characteristics

The demographic characteristics of offenders presented in Table 5.1 indicates that they are a heterogeneous group that could not be placed within a single profile, similar to findings from previous studies (e.g., Cavezza and McEwan, 2014, Dreßing et al., 2014, Maple et al., 2011). Offenders' ages ranged from 21 to 63 years with 45% being over 41 years, 35% between 31 and 40 years, and 20% between 21 and 30 years. Consistent with the finding of Dreßing et al. (2014), the majority of offenders were males (80%), yet, females were also the offender in 20% of the cases. The ethnicity of offenders varied with Middle Eastern accounting for 40%, Caucasians accounting for 35% of the cases and Far Eastern and South Asians accounting for 25%. The ethnicity findings can be based on variations in the population in the UAE. As with the professional status the majority of offenders were of middle professional status (70%), 20% were of low professional status, while 10% were unemployed.

With regards to prior offender/victim relationship (Table 5.2), the findings showed that a significant percentage were work colleagues (40%). This differed from the results of the study by Dreßing et al. (2014) where work colleagues accounted for only 6% of the offenders. The results also showed that ex-intimates accounted for 35% of offenders, which was similar to findings of a number of earlier studies (e.g.,(Cavezza and McEwan, 2014, Dreßing et al., 2014, Maple et al., 2011)). Unlike findings of Sheridan and Grant (2007), who reported that cyberstalking was mainly by acquaintances and strangers, it was observed that offenders in this study were unlikely to cyberstalk strangers (0%), or people whom they had little relationship with (10%). This was also not consistent with findings from Dreßing et al. (2014) and Maple et al. (2011) where cyberstalking strangers and acquaintances accounted for a significant amount (20.5% and 43% respectively).

The period of the cyberstalking behaviour also varied between offenders, yet, the majority lasted for six months or less (60%). 20% lasted between 7 months and a year, while 5% lasted for two years. A previous study that examined the cyberstalking duration also showed varying results, with 32% lasting for up to one month, 45.1% lasting for up to one year, and 22.8% lasting for over a year (Dreßing et al., 2014). Also, consistent with findings from Maple et al. (2011), offenders used a variation of online means to cyberstalk their victims. However, it was observed that they mainly relied on emails (personal and work), social networks, and dating websites.

The study identified seven offending behaviour themes within the sample cases (Table 5.4): (1) false accusation of victims/defamation, (2) impersonation, (3) obsession, (4) blackmailing/threatening, (5) collecting information about the victim/tracing the victim, (6) violation of privacy, and (7) extortion. Also, exploring motivations that might have influenced offender behaviour, four themes were identified (Table 5.5): (1) rejected partner seeking revenge, (2) rejected partner trying to reconcile, (3) revenge for actual or perceived injustices, and (4) monetary gain. These were similar to motivations identified by Dreßing et al. (2014), with the exception of monetary gain.

When mapping the offending behaviours and motivations with the cyberstalker typology designed by McFarlane and Bocij (2003), offenders under the rejected partner seeking revenge and rejected partner trying to reconcile in the sample exhibited behaviours that appeared to be consistent with the typology of the intimate cyberstalkers (see Chapter 2). For example, this group of offenders demonstrated having detailed knowledge about their victim. They utilised more than one electronic mean to cyberstalk their victim (e.g., email, social networks, and dating websites). Their offending behaviour involved impersonation of the victim on social networks or dating websites, defamation, and violation of privacy. Their written communication with the victim included wording that ranged from expressing love and trying to restore a broken relationship, to words of anger, rage, and threats.

The group of offenders motivated by revenge for actual or perceived injustices expressed behaviours that partially aligned with the collective cyberstalkers as defined by McFarlane and Bocij (2003). This group also utilised a number of electronic means to harass their victims. For example, they impersonated the victim on social networks and dating websites to tarnish the victim's image and reputation. They employed emails (personal and/or work) to spread embarrassing rumours or accuse the victim of false conduct. Unlike the offenders described by McFarlane and Bocij (2003) within the collective cyberstalker typology, offenders in this study sample group were always acting alone. The evidence did not indicate the involvement of more than one offender cyberstalking, or recruiting others to harass the victim offline. Also, although two of the offenders expressed/hinted on offline offending against the victim (showing an overlapping behaviour with McFarlane and Bocij (2003) vindictive and composed cyberstalkers), none of them acted upon their threats. This finding, however, could be interpreted as the offender being apprehended before having a chance to act upon their threats. Another possibility is that they were trying to frighten the victim without the intention to cause them physical harm. Yet, it is important for the DF investigator to assess the level of risk the offender pauses based on the evidence found, especially if they are unknown. Even though it is not possible to determine for definite whether the offender will escalate to offline stalking, making an assumption that is informed from the evidence can help prevent future harm.

None of the offenders exhibited a set of behaviours that significantly aligned with the vindictive cyberstalker, or the composed cyberstalker. The analysed digital evidence indicated that in all of the sample cases, offenders had specific motivations rather than harassing their victims without an apparent reason. None of the offenders used third parties or encouraged third parties to join them in their stalking. Only two of the offenders had previous convictions for physically assaulting others in offences unrelated to cyberstalking. However, it is important to recognise that most of the individuals in this study had come to the UAE from other countries, and the history of their criminal record only includes the period when they lived in the UAE.

5.9 Summary

This study continued to address the first two objectives of the programme of research: (1) examining the usability and applicability of BA in the examination, analysis, and interpretation of digital evidence, and (2) examining the ability of BA to contribute to theoretical understanding of the motivational and behavioural dynamics of computer-facilitated interpersonal crimes. It followed an abductive approach performing case-by-case examination, and applying DF analysis and BA to understand the behavioural dynamics of offenders in this crime category and related digital evidence. To address the two main objectives of the study, a number of sub questions (see Chapter 3) were identified and explored throughout the stages of the study.

The results of the research suggested that, although there are limitations associated with the use of BA, it can contribute to further understanding of the dynamics of cyberstalking crimes by mapping the digital evidence onto offending behaviour in the online environment. This is particularly useful in relation to this category of cybercrime as current knowledge about offender behaviour and investigative strategies is currently underdeveloped. It also provided structure to the investigative process, directions to potential evidence, and insight into the different interpretations of digital evidence and what it reflects with regard to offender characteristics and behaviours. The outcome of the study contributed to establishing a method for understanding the investigative utility of the different digital evidence to achieve better explanation of the events of the crime that will aid in prosecuting cyberstalking cases. Table 5.6 can assist in establishing the significance of the processed digital evidence, and help the investigator to form hypotheses about the suspect's actions. This can enable a more detailed reconstruction of evidence that can inform sentencing and prosecution.

6 A SURVEY OF PRACTITIONERS' PERCEPTIONS ON USE AND UTILITY OF BEHAVIOURAL ANALYSIS IN DIGITAL FORENSICS INVESTIGATIONS

6.1 Introduction

The results of the forensic case analyses presented in Chapter 4 and 5 showed that Behavioural Analysis (BA) appeared to complement the standard digital Forensics (DF) investigation process by aiding in the interpretation of the digital evidence, evaluating offender behaviours and motivations, and in better understanding and reconstructing crime events. However, the review of literature (Chapter 2) showed limited research and empirical testing on this issue with regards to DF investigations for computer-facilitated crimes. As such, this chapter continues the work of the previous chapters by addressing the third objective of the thesis: examining the current use and perceived evidential value of BA in policing and law enforcement.

This study empirically examined the perceptions of national and international DF practitioners regarding the use and utility of BA, including its subset BEA, during the process of investigating specific types of crimes. It focused on two crime categories: the possession and dissemination of Sexually Exploitative Imagery of Children (SEIC) and cyberstalking, as previously explored in chapters 4 and 5. It constituted the development of an online questionnaire that examined the strategies currently used in the processing of digital evidence in DF investigations. It focused specifically on the extent to which practitioners currently use activities that constituted BA in the digital evidence processing stages of SEIC and cyberstalking cases. It also addressed the perceived utility of these approaches to the DF investigation process of the associated digital evidence, and associated challenges in performing these analyses.

The term "DF practitioner" is used in a broad sense in this study; participants were from a variety of DF roles. This included analysts, examiners, investigators, first responders, data recovery engineers, managers, advisors, and consultants, as well as detective inspectors, sergeants, officers, and unit chiefs currently working in the DF field.

This chapter reports on the results of the online questionnaire. The study design, sample and related analytic strategy utilised are described in Chapter 3. The chapter is organised as follows. Section 6.2 provides a brief background of previous studies empirically evaluating the practices of different variations of BA in criminal investigations. Section 6.3 reports on the results, and section 6.4 provides a general discussion of the findings. Section 6.5 provides a summary of the chapter.

6.2 Background

A number of studies have been performed to explore the opinions of mental health professionals and police officers about the utility of criminal investigative analysis (CIA) (aka profiling) in criminal investigations. Torres et al. (2006) conducted an online survey that explored the perceived utility and the scientific merit of criminal investigative analysis among 161 forensic psychologists and psychiatrics. The main aim of the study, however, was to examine whether the naming of the investigative method as "profiling" or "criminal investigative analysis" would affect the participants perceptions of the utility, validity, and acceptance of this method. Results showed that around 10% of the participants had performed criminal investigative analysis in criminal cases. 25% reported having knowledge of this technique, and 40% thought that it was scientifically reliable. Also, the majority of the participants had a strong perception of the utility of CIA in the law enforcement context, and almost all of them believed that this technique should be researched empirically.

Snook et al. (2007) interviewed 51 police officers working in major crime divisions across Canada to examine their perspectives and beliefs in relation to CIA's utility. 57% reported having utilised CIA in criminal investigations in cases involving homicide (n=16), sexual assault (n=11), breaking and entering (n=1), and aggravated assault (n=1). Around 94% believed that CIA had utility in solving cases and 88.2% perceived it was a valuable investigative tool. 84.3% agreed that the use of CIA could help the investigator to better understand the dynamics of a case. 47.1% believed that CIA professionals could provide accurate insights on the characteristics of the offender, and 51% agreed that the skills of CIA professionals should be sought regularly when investigating criminal cases. Finally, the majority of the participants (86.3%) believed that CIA could not be applied to all types of cases, but could be useful in investigating certain categories of crimes.

A number of other earlier studies that surveyed police officers about the utility of CIA in criminal investigations showed a general acceptance of its value in investigating criminal cases (Copson, 1995, Jackson et al., 1994, Pinizzotto, 1984, Trager and Brewster, 2001). Police officers believed that CIA advanced their understanding of the case, helped open new lines of inquiry, the design interrogation strategies, and in a few cases, helped them identify the offender.

The study conducted by Torres et al. (2006) explored the utility of CIA among mental health professionals only. It explored the utility and validity of the technique in general, and did not provide any details about the categories of crimes where the technique was utilised. The other studies mentioned above surveyed police officers working in various criminal divisions without focusing on a group that worked on investigating a specific category of crime. Also, each of the previous studies focused on surveying police officers of a certain country (i.e., Canada, The United States, The United Kingdom, and the Netherlands). Further, some of the studies had a rather small sample group (e.g., six police officers), which makes the study problematic in terms of being representative of the opinions of professionals from the law enforcement community of that country. However, all of these studies provided a useful overview of how mental health professionals and police officers view the utility of CIA in relation to criminal investigations.

The literature review indicated that there have been relatively few studies empirically evaluating the practice of different variations of CIA in criminal investigations. It should also be noted that in the previous studies, the perceived utility of CIA generally focused on investigating traditional violent crimes (e.g., homicide, rape). To the best of the researcher's knowledge, there has been no study to date that examined the effectiveness of CIA in investigating digital crimes. Specifically, empirical studies that address the perceived utility of BA by digital forensics professionals do not exist at the present time.

6.3 Results

This section reports on the results of the survey.

6.3.1 General Demographics, Training and Experience

6.3.1.1 Gender

The majority of the participants were males (88.7%), while 13.3% were of the sample was female.

Gender	Number	Percent
Male	133/150	88.7%
Female	17/150	13.3%

Table 6.1 Gender of participants.

6.3.1.2 Age

The age varied across the participants ranging from 20-60+. The majority (39.7%) were within the 31-40 age group, while 2.6% were over 60 years old.

Age range	Number	Percent
20-30	40/151	26.5%
31-40	60/151	39.7%
41-50	28/151	18.5%
51-60	19/151	12.6%
60+	4/151	2.6%

Table 6.2 Age of participants.

6.3.1.3 Highest Education Level

The sample showed high levels of post-compulsory education. Most of the participants (33.7%) had a bachelor's degree, 25.1% had a master's degree, and 3.3% had a PhD. 28.8% also had a forensic professional certificate. A small percentage had a high school diploma (5.3%), and police training (4%).

Education level	Number	Percent
High school diploma	8/151	5.3%
Bachelor's degree	51/151	33.7%
Forensic professional certificate	39/151	25.8%
Police training	6/151	4%
Master's degree	38/151	25.1%
PhD	5/151	3.3%

Table 6.3 Highest level of education of participants.

6.3.1.4 Area of Primary Qualification

Over half of the participants (62.2%) had digital forensics/cyber security as their primary area of qualification. Around quarter of the participants (24.5%) were in the field of computer science and/or other fields related to information technology. 7.3% of the participants were in fields related to criminal justice, while 1.3% were in information assurance and behavioural science respectively.

Area of Primary Qualification	Number	Percent
Computer science/IT-related	37/150	24.6%
Criminal justice related	11/150	7.3%
Behavioural science	2/150	1.3%
Digital forensics/cyber security	94/150	62.6%
Accounting	1/150	0.6%
Business Administration	1/150	0.6%
Information Assurance	2/150	1.3%
Maths and physics	1/150	0.6%
Science and Education	1/150	0.6%

Table 6.4 Area of primary qualification.

6.3.1.5 Training undertaken

63.6% of the participants had attended DF certified courses (e.g., Certified Forensic Computer Examiner, Europol Open Source Linux Training). 42% had received different industrial training (e.g., EnCase, AccessData, FTK, Cellebrite). 18.5% reported their training being part of their university education, and 10% had internal trainings in their organisations.

Training	Number	Percent
University	26/140	18.5%
Digital Forensics Certified Courses	89/140	63.5%
Vendor specific courses	59/140	42%
On-the-Job Training	14/140	10%

Table 6.5 Training undertaken.

6.3.1.6 Country of Current Practice of Digital Forensics

Participants came from 36 different countries. Most of them were from the United Kingdom (17.8%), the United States (16.4%), the United Arab Emirates (8.9%), India (8.9%), South Africa (5.5%), and Australia (4.1%).

Country	Number	Percent
Algeria	1/146	0.7%
Australia	6/146	4.1%
Bahrain	1/146	0.7%
Belgium	1/146	0.7%
Bulgaria	2/146	1.4%
Canada	1/146	0.7%
Croatia	2/146	1.4%
Cyprus	2/146	1.4%
Czech Republic	2/146	1.4%
France	2/146	1.4%
Germany	4/146	2.7%
Ghana	3/146	2.1%
Greece	1/146	0.7%
India	13/146	8.9%
Ireland	1/146	0.7%
Italy	4/146	2.7%
Japan	1/146	0.7%
Jordan	1/146	0.7%
Kenya	1/146	0.7%
Kuwait	1/146	0.7%
Malaysia	1/146	0.7%
Netherlands	2/146	1.4%

New Zealand	1/146	0.7%
Oman	1/146	0.7%
Philippines	1/146	0.7%
Qatar	2/146	1.4%
Russia	2/146	1.4%
Saudi Arabia	5/146	3.4%
South Africa	8/146	5.5%
South Korea	1/146	0.7%
Spain	1/146	0.7%
Sweden	4/146	2.7%
Turkey	3/146	2.1%
United Arab Emirates	13/146	8.9%
United Kingdom	26/146	17.8%
United States	24/146	16.4%

Table 6.6 Country where participants currently practice digital forensics.

6.3.1.7 Type of Organisation Where Currently Employed

Participants were distributed almost evenly between Law enforcement (49.6%) and Private consulting firms (47.6%) in terms of current employment. 1.3% of them were self-employed.

Organisation	**Number**	**Percent**
Law enforcement	75/151	49.6%
Private consulting firm	72/151	47.6%
Self employed	2/151	1.3%

Table 6.7 Type of organisation where currently being employed.

6.3.1.8 Length of practice in the field

The majority of the participants had 8-14 years of practice (39.1%) or 2-7 years of practice (37.7%). 10.6 % had less than two years of practice, while 7.9% had 15-20 years of practice, and 4.6% had practiced in the field for over 20 years.

Years	Number	Percent
Less than 2 years	16/151	10.6%
2-7 years	57/151	37.7%
8-14 years	59/151	39.1%
15-20 years	12/151	7.9%
Over 20 years	7/151	4.6%

Table 6.8 Length of practice in the field.

6.3.1.9 Number of Different Departments Worked in

Only 139 participants answered this question. The results showed that 54.6% had been working in one department throughout their career. 17.9% worked in two different departments, 17.2% worked in three different departments, and 5.7% worked in four different departments. Also, 4.3% have worked in five or more departments.

Number of Departments	Number	Percent
One	76/139	54.6%
Two	25/139	17.9%
Three	24/139	17.2%
Four	8/139	5.7%
Five or more	6/139	4.3%

Table 6.9 Number of the different departments that the participants have worked in.

6.3.1.10 Current Job Title

The majority of the participants reported that they were DF investigators (46.8%), 11.1% were senior DF investigators, and 2.7% were junior DF investigators. 20.9% were directors of divisions, units, or departments, and 1.3% were assistant managers. 6.9% were DF consultants, 6.9% IT/Network security consultants, 2% were project managers and researchers, and 0.6% were retired.

Job title	Number	Percent
Director/ Manager/Head of Division/Unit/Department	30/143	20.9%
Assistant Manager of Division/Unit/Department	2/143	1.3%
Digital Forensics Investigator/Expert/Analyst/Examiner	67/143	46.8%
Senior Digital Forensics Investigator/Expert/Analyst/Examiner	16/143	11.1%
Junior Digital Forensics Investigator/Expert/Analyst/Examiner	4/143	2.7%
Digital Forensics Consultant	10/143	6.9%
IT/Network Security Consultant/Specialist/Analyst	10/143	6.9%
Project Manager/Researcher	3/143	2%
Retired Digital Forensics Examiner	1/143	0.6%

Table 6.10 The current job titles of the participants.

6.3.1.11 Estimated Number of Digital Forensics Investigations Performed During Career

Over a third of the participants had performed more than 300 DF investigations (36%). 14% had performed 101-200 DF investigations, 13.3% performed 51-100 DF investigations, 13.3% performed 21-50 DF investigations, while 12.7% performed 201-300 DF investigations. Also, 6% had performed 1-10 DF investigations, and 4.7% performed 11-20 DF investigations.

Number of DF investigations	Number	Percent
1-10	9/150	6.0%
11-20	7/150	4.7%
21-50	20/150	13.3%
51-100	20/150	13.3%
101-200	21/150	14.0%
201-300	19/150	12.7%
300+	54/150	36.0%

Table 6.11 Number of digital forensics investigations performed by the participants.

6.3.1.12 Types of Crimes Investigated

Most of the participants had experience investigating different kinds of crimes. The majority had investigated fraud (91.5%), 79.7% had investigated hacking, 73.9% worked on SEIC cases, and 62.15% investigated cyberstalking cases. A little over half of the participants had experiences investigating assault cases (52.9%), while 56.9% investigated robbery, and 49% had worked on cases of rape. Also, a little under half of the participants have experienced investigating copyright infringement (47.1%), electronic money laundering (44.4%), cyber terrorism (43.1%), homicide (41.8%), and software piracy (35%). The other categories had relatively smaller frequencies of investigations.

Type of crime	**Number**	**Percent**
Homicide	89/153	41.8%
Rape	75/153	49%
Assault	81/153	52.9%
Robbery	87/153	56.9%
Fraud	140/153	91.5%
Hacking	122/153	79.7%
SEIC	113/153	73.9%
Cyberstalking	95/153	62.1%
Copyright infringement	72/153	47.1%
Software piracy	54/153	35%
Electronic money laundering	68/153	44.4%
Cyber terrorism	66/153	43.1%
Narcotics and drug trafficking	5/153	3.2%
Counterfeit/forgery	5/153	3.2%
Employee misconduct/misuse of privileges	6/153	3.9%
Civil/domestic litigation	2/153	1.3%
Identity theft	3/153	1.9%
Kidnapping/Missing persons	2/153	1.3%
Suicide	1/153	0.6%
Adult Pornography	1/153	0.6%

Table 6.12 Types of crimes that have been investigated.

6.3.1.13 Use of Specific Digital Forensics Methodologies or Protocols When Performing Digital Forensics Investigations

The majority of the participants (86.7%) followed a specific DF methodology or protocol when performing DF investigations. 13.3% reported that they did not follow any specific methodology.

6.3.2 General Awareness and use of BEA

This section reports on participants responses with regard to their general knowledge of BEA and its utilisation in DF investigations.

6.3.2.1 Knowledge of BEA

47.7% reported that they were aware of what BEA is and had some knowledge about it, while 52.3% reported that they did not know what it was.

6.3.2.2 Awareness of Utilisation of Different BEA Strategies in Digital Forensics Investigations

Out of the participants that were aware of BEA, 78.9% reported having knowledge of the different strategies of BEA that can be utilised in DF investigations, while 21.1% reported not being aware of these strategies.

6.3.2.3 Utilising BEA in Digital Forensics Investigations

52.1% of the participants who reported being aware of BEA also reported that they had utilised BEA in digital forensics investigations. On the other hand, 47.9% reported not using BEA.

6.3.2.4 Comments and insights on the utility of BEA

Participants were asked to provide their perceptions of the utility of BEA in digital forensics investigations. 30 responses were obtained. Their answers were analysed thematically, and the responses were categorised into two themes: utility of BEA, and factors limiting the use of BEA. Participants believed that BEA can be useful in a DF investigation in a number of ways. One respondent perceived that it reduces the number of suspects and shortens the time of the investigation. Others believed that it provides guidance, links, and directions on where to look for evidence, insight into behaviour and motivation of the offender, and in designing interrogation strategies. Table 6.13 summarised the identified utility of BEA as described by participants.

Utility of BEA	Quotes from the participants' answers
Reduces the number of suspects	▪ *BEA has been useful in reducing the number of suspects in an investigation..*
Shortens time of investigation	▪ *BEA has been useful… by shortening the period of time it takes in solving a case.*
Provides guidance, links, and directions on where to look for evidence	▪ *… it guide[s] you to reach the fact[s].* ▪ *… provides several 'markers' to suggest their behaviour warrants further investigation and also provides a number of different lines of analysis.* ▪ *Profiling the behavior of someone outside the web can be very insightful into finding electronic evidence.* ▪ *It is to capture the behaviour of the suspect to ensure I am able to get the evidence, or what type of digital evidence can be seen (prediction based) and directly find for relevant evidence.*
Helps with reconstruction of the crime events	▪ *.. to help us establish and understand the picture as a whole.*
Provides insights on the probable offender	▪ *[in SEIC cases] …monitor the suspects activity online… Question yourself is it really the suspect the one who is in control of his/her computer during the download and sharing?*
Provides insights on the behaviour and motivation of the offender	▪ *… gaining insight into their motivation…* ▪ *I was able to find many information on the behaviour of people involved in crimes by analysing their activities on social networks.* ▪ *behavioral analysis of this nature can offer deep insights concerning victim and offender pathology.*
Helps understand the psychological state of the offender to suggest further evaluation/treatment	▪ *We compare our profile of the client to the findings in the evidence and facts of the case… We can use these findings to discuss our results and theories with the attorney, who then may suggest the client undergo a psycho-sexual evaluation.* ▪ *… offers a unique insight into their mental state, like[s], dislikes and actions.*
Helps in designing interrogation strategies	▪ *I have mostly used the BEA when interviewing offenders to obtain confessions by gaining insight into their motivations…*
Useful in certain situations and categories of crime.	▪ *Can be useful in cyber-stalking, child molestation, certain frauds…* ▪ *Some instances or types of crimes especially those around exploitation of children etc. usually have a more defined BEA.* ▪ *In cases of Incident response, BEA very helpful for investigation.*
Provides clearer crime explanations to legal representatives	▪ *We took this to another level when working with offenders and their legal representatives.*

Table 6.13 Participant perspectives on the utility of BEA.

Participants also provided some insight into the factors that limits the use of BEA in DF investigations. Among these were the lack of proper knowledge of BEA, resource constraints, and cases lacking of sufficient digital evidence that reflect behaviours of the involved individuals. Table 6.14 summarises the identified factors and provides illustrative quotes from the participants' responses.

Limiting factors of utilising BEA	Quotes from the participants' answers
Lack of proper knowledge of BEA	▪ *Unfortunately most digital investigators are not well equipped with BEA knowledge…* ▪ *Ironically most seasoned digital forensic practitioners perform BEA to a basic level as a developed skill in their role.* ▪ *The skills required to interpret BEA indicators derived from digital forensic analysis performed on devices is very different from the technical skills needed to undertake extraction of evidence.* ▪ *I am familiar with a term BEA, but not how it is implemented into Forensic investigations.* ▪ *Should be carried out by experiences and well trained people.*
Resource constraints	▪ *Limiting factors of using BEA in DF is time and money.*
Cases lacking of sufficient digital evidence that reflect behaviours of the involved individuals	▪ *An investigator must utilise knowledge of a character, if it is available, to understand how they might conceal any hidden truths. Character details is usually not available, so usually I would not be able to utilise BEA* ▪ *Some instances or types of crimes... usually have a more defined BEA. Some other crimes are not always as easy to define.*

Table 6.14 Identified factors that limit the use of BEA.

6.3.3 Behavioural Analysis use and utility in relation to SEIC

6.3.3.1 Experience of investigating SEIC cases

Most of the participants (74.8%) had investigated SEIC cases.

6.3.3.2 Estimation of Number of Digital Forensics Investigations Performed for SEIC Cases.

The majority of the participants who had investigated SEIC cases had been involved in over 50 cases (37.2%). 16.8% had investigated 21-50 cases, 13.3% had investigated 11-20 cases, 13.3% hade investigated 6-10 cases, and 19.5% had investigated 1-5 cases.

Number of DF investigations on SEIC cases	Number	Percent
1-5	22/113	19.5%
6-10	15/113	13.3%
11-20	15/113	13.3%
21-50	19/113	16.8%
over 50 cases	42/113	37.2%

Table 6.15 Number of digital forensics investigations on SEIC cases.

6.3.3.3 Utilisation of Behavioural Analysis Activities in Investigations of SEIC Cases

This scale measured usage of activities that constitute BA while investigating SEIC cases. The results indicated that over half of the participants (53.6%) always performed a quick review of the available electronic evidence when investigating these cases, and 33.9% performed it most of the time. 35.7% always performed a critical assessment of the hypotheses and conclusions made by other investigators, and 23.2% performed it sometimes. Moreover, most of the participants (38.7%) always looked for electronic evidence reflecting the behaviour of the offender in an attempt to understand their motivations. 22.5% performed this activity most of the time.

Almost three quarters of the participants (73%) always looked for electronic evidence indicating how the offender obtained SEIC material, with 23.4% performing this activity most of the time. A little over half of the participants (51.4%) always looked for electronic evidence indicating the relationship between the victim and offender, and 19.8% performed this activity most of the time. Finally, 41.4% always performed a timeline analysis in an attempt to reconstruct the probable sequence of the events of the crime, and 27% performed this most of the time.

Activities that constitute BA	**Never**	**Rarely**	**Sometimes**	**Most of the time**	**Always**
Perform a quick review of the available electronic evidence.	-	2.7% (3/112)	9.8% (11/112)	33.9% (38/112)	53.6% (60/112)
Perform a critical assessment of the hypotheses and conclusions made by other investigators	6.3% (7/112)	12.5% (14/112)	23.2% (26/112)	22.3% (25/112)	35.7% (40/112)
Look for electronic evidence that reflects the behaviour of the offender in an attempt to understand their motivations	7.2% (8/111)	13.5% (15/111)	18% (20/111)	22.5% (25/111)	38.7% (43/111)
Look for electronic evidence that indicates how the offender obtained the child pornography material	-	-	3.6% (4/111)	23.4% (26/111)	73% (81/111)
Look for electronic evidence that indicates the relationship between the victim and offender	1.8% (2/111)	4.5% (5/111)	19.8% (22/111)	19.8% (25/111)	51.4% (57/111)
Perform a timeline analysis in an attempt to reconstruct the probable sequence of the events of the crime	0.9% (1/111)	7.2% (8/111)	23.4% (26/111)	27% (30/111)	41.4% (46/111)

Table 6.16 Using activities that constitute BA while investigating SEIC cases.

6.3.3.4 Examining the Perceived Utility of Behavioural Analysis in Relation to Investigating SEIC Cases

This scale measured the perceived utility of BA in relation to investigating SEIC cases. 42.3% strongly agreed that knowing the suspect's technical skills would help to determine where to

look for digital evidence. 77.4% strongly agreed or agreed that interpreting the behaviour of the offender from the electronic evidence could provide more knowledge about their motivations. Also, 77.5% strongly agreed or agreed that interpreting the behaviour of the offender from the electronic evidence could provide more knowledge about their psychological state. Moreover, 65.7% strongly agreed or agreed that interpreting the behaviour of the offender from the electronic evidence could provide more knowledge about risk of reoffending and involvement in other criminal activity. Further, 77.5% strongly agreed or agreed that interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the circumstances of the crime. Finally, 81.4% strongly agreed or agreed that interpreting the behaviour of the offender from the electronic evidence could provide more knowledge about the sequence of the crime events.

When examining the participants' agreement with the statement "interpreting the behaviour of the offender from the electronic evidence would not be useful", 79.3% strongly disagreed or disagreed. 14.4% were uncertain, and 6.3% agreed or strongly agreed with the statement. Also, 58.5% strongly agreed or agreed that they perform the examination of the electronic evidence based exactly on what is asked in the request letter/terms of reference/warrant. 11.7% were uncertain, and 29.7% disagreed, or strongly disagreed. Finally, 43.5% strongly disagreed or disagreed that conducting further analysis on the behaviour of the offender would not be an effective use of time, resources, and effort. 39.1% were uncertain, and 16.3% strongly agree or agreed.

Statement	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
Knowing the suspect's technical skills will help me to determine where to look for digital evidence	1.8% 2/111	8.1% 9/111	4.5% 5/111	43.2% 48/111	42.3% 47/111
Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about their motivations	-	3.6% 4/111	18.9% 21/111	49.5% 55/111	27.9% 31/111
Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about their psychological state	-	4.5% 5/111	27.9% 31/111	45.9% 51/111	21.6% 24/111
Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the risk they pose for reoffending, involvement in other criminal activity, etc	0.9% 1/111	3.6% 4/111	29.7% 33/111	48.6% 54/111	17.1% 19/111
Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the circumstances of the crime	-	1.8% 2/111	20.7% 23/111	55.9% 62/111	21.6% 24/111
Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the sequence of the crime events	-	1.8% 2/111	17.1% 19/111	59.5% 66/111	21.6% 24/111
Interpreting the behaviour of the offender from the electronic evidence would not be useful	27.9% 31/111	51.4% 57/111	14.4% 16/111	5.4% 6/111	0.9% 1/111
Perform the examination of the electronic evidence based exactly on what is asked in the request letter/terms of reference/warrant	4.5% 5/111	25.2% 28/111	11.7% 13/111	38.7% 43/111	19.8% 22/111
Conducting further analysis on the behaviour of the offender would not be an effective use of time, resources, and effort	11.8% 13/110	31.7% 36/110	39.1% 43/110	14.5% 16/110	1.8% 2/110

Table 6.17 Examining the perceived utility of BA in investigating SEIC cases.

6.3.3.5 Challenges Faced During the Digital Forensic Investigation of SEIC Cases in Terms of the Examination of the Electronic Evidence

Participants were asked to provide their perceptions of the challenges that they face during the DF investigations of SEIC cases in terms of the examination of the electronic evidence. 92 participants answered this question. Their answers were analysed thematically, challenge themes were identified. The themes were categorised into SEIC specific challenges, and generic challenges that affect SEIC investigations. The SEIC specific challenges included four themes: (1) establishing nature/degree of the offence, (2) difficult identification of suspects/victims, (3) stressful working conditions for SEIC examiners, and (4) non-standardised operations and legal framework. Table 6.18 summarised the identified categories and provides illustrative quotes from the participants.

Challenges	Quotes from the participants' answers
Establishing nature/degree of the offence	▪ *Trying to determine if the suspect is a trafficker or mere collector.* ▪ *Prove if the suspect published videos and pictures on the internet through p2p programs.* ▪ *Did the user spread material. If yes how much and to who?* ▪ *How much material?*
Difficult identification of suspects/victims	▪ *To identify the real ID of the victims to discover if there are more victims* ▪ *Trying to determine if there is an identifiable victim..* ▪ *Agreeing/disagreeing on whether a young-looking person is definitely underage.* ▪ *Determine whether it is a child or not…* ▪ *… determination of the true age of victims…*
Stressful working conditions for SEIC examiners	▪ *Staying unemotional in a case where a child had been abused to that extent is very cumbersome.* ▪ *Images of child abuse can be very disturbing and lead to negative impacts on the health of investigators.* ▪ *Prolonged exposure to obscene material may create mental health issues for investigators, prosecutors, and forensic interrogators.*
Non-standardised operations and legal framework	▪ *[COPINE scale] not being recognised… means only more serious and obvious types of CP are considered/prosecuted.* ▪ *There is a need for regional and national standard operating procedures in relation to the discovery of indecent images by private sector investigations.*

Table 6.18 SEIC specific challenges faced during DF investigation of SEIC cases.

Challenges	Quotes from the participants' answers
Evolution of technology and offender's skills	▪ *Anti-forensics actions.* ▪ *Complexity of the encryption...* ▪ *Steganography/cryptography are the biggest challenges.* ▪ *Ineffectiveness in tracing criminal activity when data nonymization and obfuscation techniques have been employed.* ▪ *Electronic devices are changing all the time… the software used needs to be constantly updated to obtain the data from the devices.* ▪ *Storage of images and data being held in 'the cloud' is becoming more difficult to manage an offender having access even when devices are seized.*
Increasing volume of data to be investigated	▪ *Excessive quantity of picture/video files to review and/or categorise.* ▪ *Many photos and videos to tag.* ▪ *…dealing with a large data set.* ▪ *… slow processing times on large data sets…* ▪ *Large data sets, increased time to perform categorization* ▪ *The quantity of data to be reviewed, if it were to be done properly, is too great for the time and funding available.* ▪ *Back log and time available to complete the task.* ▪ *Slow processing times on large data sets.*
Evidence handling, analysis and reporting	▪ *actually we get evidence colected by law enforcement or other customer mostly done without correct procedure, often it is contaminated..* ▪ *Lack of knowledge in gathering the actual evidence.* ▪ *the problem we have on a regular occurrence is that officers do not understand the four principles of the ACPO guidelines for digital evidence.* ▪ *Thumbnail pictures can be a pain, very little detail.* ▪ *Known hash sets are over relied upon.*
Limited resources available	▪ *The frequency of child pornography cases is increasing compared to the available resources to combat the situation.* ▪ *..there is a huge amount if backlog of digital forensics cases building up at police stations. Thus more forensics personnel are required.* ▪ *Our scope of information and resources can be very limited.* ▪ *The time required for grading of electronic items is extensive and sometimes prohibits a deeper analysis.* ▪ *There are restrictions on timing and funding that would restrict the remit of many investigations.*
Lab management and commission of cases	▪ *Investigations derailed in policing environment when non-technical managers are appointed to supervisory positions without substantive experience overseeing inquiries into child pornography or attending to the rigors of digital forensic casework.* ▪ *Police forces do not like higher invoices than the quoted for, so spending extra time on cases rarely happens, its all money related, sadly.* ▪ *Lack of information or guidance from those requesting the work.* ▪ *Lack of technical knowledge of those requesting the work, and the lack of willingness to learn/hear about it.*
Insufficient cooperation	▪ *It was difficult to get access to the necessary information/data especially stored in foreign country.* ▪ *Lack of cooperation from different organizations and abroad companies.* ▪ *Information sharing between prosecution and defence needs attention.*

Table 6.19 General challenges faced during the DF investigation of SEIC cases.

6.3.3.6 Suggestions to Improve the Digital Forensic Investigation of SEIC Cases

Participants were asked to provide their suggestion on ways to improve DF investigations of SEIC cases. 80 participants answered this question. Their answers were analysed thematically, and six themes were identified. Among these were to utilise behavioural analysis, employ triage techniques, training, and proper interrogations of victims and offender. Table 6.20 summarises the identified categories and provides illustrative quotes from the respondents.

Suggestions for improvement	**Quotes from the participants' answers**
Utilise behavioural analysis	▪ *I believe that trying to understand motivation is important.* ▪ *[Understand suspect's] behaviour patterns.* ▪ *More cooperation with physiological doctors.* ▪ *Never trust the forensic software tool alone..instinct and common sense works very well.*
Employ triage techniques	▪ *Triaging evidence first and looking for relevant evidence of CP, then doing a deeper dive.* ▪ *Very good triage techniques.* ▪ *Triage process to be done by police beforehand.*
Training of digital investigators/practitioners and members of the legal system	▪ *Police must … be trained in industry best practices for handling electronic evidence.* ▪ *Train investigators to obtain more information from the first encounter of the suspect* ▪ *Better training for examiners and investigators.* ▪ *[Members of the legal system] must be provided with ongoing training which is focused on modes of criminal offending… emerging sources of electronic information, and communication technologies.*
Proper interrogation of suspects and victims	▪ *Proper Interrogation of Suspect and victim* ▪ *Great interrogation skills*
Provide sufficient resources	▪ *More time or funding when necessary.* ▪ *Police must be equipped with the latest technology…* ▪ *Affordable tools and equipment so that small departments like mine can afford to obtain the best software and equipment in investigating these types of crimes* ▪ *Updated digital forensic tools.* ▪ *more forensics personnel are required.* ▪ *More staff to complete the work faster.* ▪ *To build multidisciplinary teams… to encourage… retention of talent.*
Overcome technical challenges	▪ *Database of known images and their classification - as per the International Scale (1 to 5).* ▪ *A worldwide database.* ▪ *More and easier sharing of hash sets of [SEIC] images* ▪ *A unique global database of hash values (photos of child pornography).* ▪ *Invent something to clear up tiny pictures.* ▪ *Having an option to be able access 'cloud' storage to gain further evidence*

Table 6.20 Suggestions to improve the digital forensic investigation of SEIC cases.

6.3.4 Behavioural Analysis Use and Utility in Relation to Cyberstalking

6.3.4.1 Experience in investigating cyberstalking cases

Over half of the participants (59.7%) had investigated cyberstalking cases.

6.3.4.2 Estimation of the number of digital forensics investigations performed on cyberstalking cases.

Most of the participants who have had investigated cyberstalking cases have investigated 1-5 cases (36.4%). 22.7% have investigated 6-10 cases, 14.8% have investigated 11-20 cases, 13.6% have investigated 21-50 cases, and 12.5% have investigated over 50 cases.

Number of DF investigations on cyberstalking cases	Number	Percent
1-5	32/88	36.4%
6-10	20/88	22.7%
11-20	13/88	14.8%
21-50	12/88	13.6%
Over 50 cases	11/88	12.5%

Table 6.21 Number of DF investigations on cyberstalking cases.

6.3.4.3 Utilisation of BEA Activities in Investigations of Cyberstalking Cases

This scale measured usage of activities that constitute BA while investigating cyberstalking cases. Results showed that 46% always performed a quick review of the available electronic evidence when investigating cyberstalking cases, and 37.8% performed it most of the time. Also, 31.8% always performed a critical assessment of the hypotheses and conclusions made by other investigators, and 34.1% perform it most of the time. Moreover, 30.7% of the participants always look for electronic evidence that reflects the behaviour of the offender in an attempt to understand their motivations, and 36.4% perform this activity most of the time.

Further, half of the participants (50%) always look for electronic evidence that indicates the relationship between the victim and offender, and 39.8% perform this activity most of the time. Also, in cases were the victim and offender were not already known to each other, 36% reported that they always look for electronic evidence that reflects the victim's behaviour that may have put them at risk of victimisation, and 37.2% perform this activity most of the times. Finally, 46% always perform a timeline analysis in an attempt to reconstruct the probable sequence of the events of the crime, and 33.3% perform this most of the time.

Activities that constitute BA	Never	Rarely	Sometimes	Most of the time	Always
Perform a quick review of the available electronic evidence.	1.1% (1/87)	1.1% (1/87)	13.8% (12/87)	37.8% (33/87)	46% (40/87)
Perform a critical assessment of the hypotheses and conclusions made by other investigators	2.3% (2/88)	5.7% (5/88)	26.1% (23/88)	34.1% (30/88)	31.8% (28/88)
Look for electronic evidence that reflects the behaviour of the offender in an attempt to understand their motivations	2.3% (2/88)	5.7% (5/88)	25% (22/88)	36.4% (32/88)	30.7% (27/88)
I look for electronic evidence that indicates the relationship between the victim and offender (e.g., written communication)	-	3.4% (3/88)	6.8% (6/88)	39.8% (35/88)	50% (44/88)
If the victim and offender were not already known to each other, I look for electronic evidence that reflects the victim's behaviour that may have put them at risk of victimisation (e.g., web browsing activities)	3.5% (3/86)	10.5% (9/86)	12.8% (11/86)	37.2% (32/86)	36% (31/86)
Perform a timeline analysis in an attempt to reconstruct the probable sequence of the events of the crime	2.3% (2/87)	3.4% (3/87)	14.9% (13/87)	33.3% (29/87)	46% (40/87)

Table 6.22 Using activities that constitute BA while investigating cyberstalking cases.

6.3.4.4 Examining the Perceived Utility of BA in Relation to Investigating Cyberstalking Cases

This scale measured the perceived utility of BA in relation to investigating cyberstalking cases. 87.4% strongly agreed or agreed that knowing the suspect's technical skills would help to determine where to look for digital evidence. Also, 78.2% strongly agreed or agreed that interpreting the behaviour of the offender from the electronic evidence could provide more knowledge about their motivations. Furthermore, 66.7% strongly agreed or agreed that interpreting the behaviour of the offender from the electronic evidence could provide more knowledge about their psychological state. Moreover, 75.6% strongly agreed or agreed that interpreting the behaviour of the offender from the electronic evidence could provide more knowledge about the risk they pose for reoffending, involvement in other criminal activity, etc. Further, 81.4% strongly agreed or agreed that interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the circumstances of the crime. Also, 83.8% strongly agreed or agreed that interpreting the behaviour of the offender from the electronic evidence could provide more knowledge about the sequence of the crime events. Finally, 71.9% strongly agreed or agreed that interpreting the behaviour of the victim from the electronic evidence could provide more knowledge about what placed them at risk of victimisation.

When examining the participants' agreement with the statement "interpreting the behaviour of the offender from the electronic evidence would not be useful", 70.5% strongly disagreed or disagreed. 16.3% were uncertain, and 12.8% strongly agreed or agreed. Also, 54.1% strongly agreed or agreed that they perform the examination of the electronic evidence based exactly on what is asked in the request letter/terms of reference/warrant. 17.6% were uncertain, and 28.5% disagreed or strongly disagreed. Finally, 52.3% strongly disagreed or disagreed that conducting further analysis on the behaviour of the offender would not be an effective use of time, resources, and effort. 30.2% were uncertain, and 17.5% agreed or strongly agreed.

Statement	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
Knowing the suspect's technical skills will help me to determine where to look for digital evidence	1.1% (1/87)	4.6% (4/87)	6.9% (6/87)	52.9% (46/87)	34.5% (30/87)
Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about their motivations	-	5.7% (5/87)	16.1% (14/87)	57.5% (50/87)	20.7% (18/87)
Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about their psychological state	-	8% (7/87)	25.3% (22/87)	50.6% (44/87)	16.1% (14/87)
Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the risk they pose for reoffending, involvement in other criminal activity, etc.	-	5.8% (5/86)	18.6% (16/86)	59.3% (51/86)	16.3% (14/86)
Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the circumstances of the crime	-	1.2% (1/86)	17.4% (15/86)	57% (49/86)	24.4% (21/86)
Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the sequence of the crime events	-	1.2% (1/86)	15.1% (13/86)	60.5% (52/86)	23.3% (20/86)
Interpreting the behaviour of the victim from the electronic evidence can provide more knowledge about what placed them at risk of victimisation	-	4.7% (4/85)	23.5% (20/85)	56.5% (48/85)	15.3% (13/85)
Interpreting the behaviour of the offender from the electronic evidence would not be useful	22.1% (19/86)	48.8% (42/86)	16.3% (14/86)	9.3% (8/86)	3.5% (3/86)
Perform the examination of the electronic evidence based exactly on what is asked in the request letter/terms of reference/warrant	2.4% (2/85)	25.9% (22/85)	17.6% (15/85)	37.6% (32/85)	16.5% (14/85)
Conducting further analysis on the behaviour of the offender would not be an effective use of time, resources, and effort	9.3% (8/86)	43% (37/86)	30.2% (26/86)	12.8% (11/86)	4.7% (4/86)

Table 6.23 Examining the perceived utility of BA in investigating cyberstalking cases.

6.3.4.5 Challenges Faced During the Digital Forensic Investigation of Cyberstalking Cases in Terms of the Examination of the Electronic Evidence

Participants were asked to provide their perceptions of the challenges that they face during the DF investigations of cyberstalking cases in terms of the examination of the electronic evidence. 63 participants answered this question. Their answers were analysed thematically, and challenge themes were identified. The themes were categorised into cyberstalking specific challenges, and generic challenges that affect cyberstalking. The cyberstalking specific challenges included four themes: (1) establishing events of the offence, (2) difficult identification of suspects, (3) obtaining inaccurate statement from victims, and (4) lack of standardised international laws. Tables 6.24 and 6.25 summarise the identified categories and provide illustrative quotes from the participants.

Challenges	**Quotes from the participants' answers**
Establishing events of the offence	▪ *it was difficult to understand the links between suspect's virtual / internet personalityes that he uses for.* ▪ *in cyberstalking it is always hard to know what is the point where offender has crossed the line and became an enemy…* ▪ *trying to establish the sequence of the crime events.* ▪ *Reconstruction of event.*
Difficult identification of suspects	▪ *not always to find the person behind the crime.* ▪ *prove what was done and by whom.*
Obtaining inaccurate statement from victims	▪ *dishonest statements by victims.* ▪ *Often they [the victims] won't admit what predicated the stalking* ▪ *These cases frequently involve a victim who is either inarticulate or incorrect regarding many of the facts of the case.*
Lack of standardised international laws	▪ *Legislative provisions which are not harmonized among members of the international community may create safe jurisdictions for cyber-stalking offending, and possible conflicts of law.*

Table 6.24 Cyberstalking specific challenges faced during the DF investigation of cyberstalking cases.

Challenges	Quotes from the participants' answers
Evolution of technology and offender's skills	▪ *Ineffectiveness in tracing criminal activity when data anonymization and obfuscation techniques have been employed.* ▪ *Anonymous services on the Internet (e.g., difficulties in identifying the suspect)* ▪ *The stalkers can use so many proxy connections and constantly change user name.* ▪ *Use of faked/temp email services. Used of Gmail and faked FB.* ▪ *the digital knowledge of the offender in decryption.* ▪ *The majority of offenders have advanced experience with IT technologies and use professional tools to protect their data and possible evidence.* ▪ *The frequency of change in social internet applications and keeping ahead of the game.* ▪ *Inability to obtain authorization for conducting online inspection and collection of remotely stored data, particularly if the target host is a cloud service provider…* ▪ *cloud based evidence.* ▪ *Cyber cloud investigation*
Increasing volume of data to be investigated	▪ *Inability to expediently locate relevant information amongst large sets of data.* ▪ *Size of storage.*
Insufficient cooperation	▪ *co-op. with other parties i.e., ISP & Law enforcement.* ▪ *Hard to get information from certain apps/companies.* ▪ *Obtaining supporting info from 3rd parties such as Facebook, Google, etc.* ▪ *Obtaining production orders against ISPs could prove a challenge.* ▪ *Slowness of responses from ISPs.* ▪ *Strict and formal international mechanisms of cooperation may impede the agility of police investigations which target cyber-stalking offending originating outside national borders.* ▪ *jurisdictions and dealing with international authorities.* ▪ *getting relevant data and evidence from location out of local jurisdiction.* ▪ *Lack of proper Intel from investigating officers.*
Limited resources	▪ *time/financial constraints.* ▪ *Limited time and congestion of cases.*

Table 6.25 General challenges faced during the DF investigation of cyberstalking cases.

6.3.4.6 Suggestions to Improve the Digital Forensic Investigation of Cyberstalking Cases

Participants were asked to provide their suggestion on ways to improve DF investigations of cyberstalking cases. 57 participants answered this question. Their answers were analysed thematically, and Table 6.26 presents the identified categories.

Suggestions for improvement	Quotes from the participants' answers
Special investigators for cyberstalking cases	▪ *There should be a special investigator that focuses on cyberstalking.*
Review of legislations	▪ *Legislation must give greater attention to the realities of the function performed by police and the impact that technology exerts upon investigations, forensic inquiries and prosecutions.* ▪ *enforcing legislation to compel cooperation by suspects also assists in neutralizing some of the impact of encryption* ▪ *Review laws to better reflect the current state of technology.* ▪ *Legislation changes which allow law enforcement access to otherwise unreachable content would be useful.*
Using best practices in evidence seizer	▪ *Best practice in evidence seizure.*
Standardisation	▪ *International level agreement.*
Overcoming jurisdiction boundaries	▪ *Easier methods of accessing information from outside jurisdiction.*
Ongoing training of members of the legal system.	▪ *improvement in law enforcement capabilities especially in understanding technology* ▪ *extensive training across the board* ▪ *training is critically needed to educate senior managers in law enforcement agencies about the utility and function of digital forensics investigations.* ▪ *improved cognizance about what investigators and prosecutors can and cannot achieve in relation to countering cyber-stalking and convicting offenders.*
Ongoing training of digital investigators/practitioners	▪ *better training for investigators and examiners.* ▪ *train those who conduct the investigation in digital forensics*
Assign sufficient time for examination	▪ *Additional time.* ▪ *More time for a deep investigation.*
Providing sufficient examination tools and equipment	▪ *better tools*
Provide sufficient information regarding the case from the requesting party	▪ *Getting more information.* ▪ *More details.* ▪ *Provide more details about the case.*
Prioritising cases	▪ *screening policies should be employed to avoid wasteful expenditure of resources on non-critical or immaterial cyber-stalking cases.*
Effective collaboration between the parties involved in the investigation	▪ *Social media platforms should be more cooperative and flag abusive behaviour.* ▪ *Ability to move quickly to obtain data from the ISPs and telephone providers.* ▪ *More co-operation with various service providers* ▪ *More cooperation from social network service providers to aid investigations.* ▪ *More support from chat providers.*
Effective communication between digital forensic investigators/practitioners globally	▪ *The forensic team needs to be able to interact with many other professionals to may obtain information and knowledge about different technologies and practices*
Utilising behavioural analysis	▪ *Looking at motivation. Also the technical capability of the stalker.*

	▪ *Creating a statistical database of behavioral evolution of offender.* ▪ *Interpreting the relationship between the offender and the victim.* ▪ *Having some studies at your hand that give you an idea about what psychologically interesting findings/hints might be helpful to profile an offender would be nice to have.* ▪ *That might be of high interest… to a psychologist or criminalist for evaluating the offenders state of mind and the risk that he might pose in real life.* ▪ *Profiling the victim and the suspect.* ▪ *Understanding the state of mind of the victim…*
Proper interrogation of suspects and victims	▪ *Working on interviewing techniques with the officers who initiate the investigations.* ▪ *Solid victim interviews.*

Table 6.26 Suggestions to improve the DF investigation of cyberstalking cases.

6.4 Discussion

This study aimed to explore the perceptions of national and international DF practitioners on the use and utility of BA, including its subset BEA, during the process of investigating digital crimes that involve SEIC and cyberstalking.

When asking about knowledge and application of BEA in general, 47.7% reported having knowledge of BEA (with 78.9% of them reporting being aware of BEA's different strategies). Also, a number of ways in which BEA has investigative benefits were identified by participants. Among these were reducing the number of suspects, shortening investigation time, and providing investigative guidance, links and directions. Providing insights on perpetrator motivations and psychological states, as well as informing the design of interrogation strategies, were also mentioned. These benefits are consistent with findings from earlier studies that surveyed the utility of BA in investigating traditional crimes (Copson, 1995, Jackson et al., 1994, Pinizzotto, 1984, Snook et al., 2007, Trager and Brewster, 2001). Responses also indicated the specific utility of BEA as an investigative tool in specific types of crimes such as cyberstalking, SEIC, and other crimes that involve human communication. This was consistent with the earlier study by Snook et al. (2007). Participants also encouraged integrating BEA within the DF investigation process:

> *Have thought from the early days of digital forensics that BEA should play a major role [in DF investigations].*

> *We really need to improve all areas of Forensic[s] and the introduction of new methodologies and approaches. Especially in the digital and computer*

> *Forensic[s]… in terms of the intersection of information technology with classic criminology.*

Although most of the participants (86.7%) had a technical background and expertise, they had a strong perception of BA as a useful investigative tool if combined with standard DF processes. Measuring the perceived utility of BA in relation to investigating SEIC cases showed that an average of 76.2% of the participants either agreed with all the statements that described the different utilities of BA in investigating SEIC crimes. Similarly, an average of 76.9% of the participants agreed with all the statements that described the different utilities of BA in investigating cyberstalking crimes. This supported earlier studies that showed that BA could be a significant investigative tool in investigating specific types of computer-facilitated crimes (Rogers and Seigfried-Spellar, 2014, Silde and Angelopoulou, 2014).

Despite the identified utility of BA, only a little over half of the participants (the 47% who reported having knowledge of BEA) reported having ever utilised BEA in DF investigations. A question that emerged from this finding was why would DF investigators who reported having knowledge of BEA did not utilise it in their investigations? One possible interpretation is that the idea of utilising behavioural analysis to assist in DF investigations has only recently been developed (Casey, 2002, Turvey, 2011). A number of published studies have been conducted in this area (e.g., Casey, 2011, Rogers, 2003, Rogers, 2015, Shaw, 2006, Silde and Angelopoulou, 2014), however, it is still a developing field that requires more scientific research. Further, very little empirical work has been conducted in this area to demonstrate the benefits of behavioural analysis in assisting DF investigations to specific categories of crimes (e.g., Rogers and Seigfried-Spellar, 2014). The lack of scientific research, clear methodologies on integrating BA with DF investigations, studies of pragmatic value, and empirical research with more definitive results on the practical value and application of BA might have prevented DF practitioners from utilising BEA in their investigations. This interpretation was also supported by the input of a number of participants who mentioned the lack of proper knowledge about BEA among DF practitioners, and only having a very basic understanding of it.

> *It is an emerging field, though some contend that it lacks sufficient scientific certainty.*

> *Unfortunately most digital investigators are not well equipped with BEA knowledge.*

> *I am familiar with a term BEA, but not how it is implemented into Forensic investigations.*

Another interpretation, which was inferred from participants' input, was that DF practitioners are always restricted by two main factors: time, and money. DF practitioners are usually pressured into performing the DF investigation process within a restricted time frame. In many of the cases, integrating BA within the DF process would exhaust the available resources. Interestingly however, 43.5% and 52.3% of participants who investigated SEIC, and cyberstalking cases respectively disagreed that performing further behavioural analysis in a case would not be an effective use of time, resources, and effort. Still, a considerable percentage of participants (39.1% and 30.2% of SEIC and cyberstalking investigators) were uncertain about this statement, which suggests that there still is an issue of weighing the benefits of utilising BA against other restricting factors, and being unable to decide whether it is worth performing or not.

A third interpretation was that the cases that were investigated did not have the kind of evidence needed to perform BA. A DF professional can only perform BA in cases where there is evidence from which to extract information on the offender and victim behaviours (e.g., written communications, history of Internet activities). It is possible that offenders and victims in the cases investigated by the respondents did not exhibit sufficient evidence on their behaviours. It is also possible that the types of cases were not of those that included sufficient personal interactions between offenders and victims to enable the DF investigator perform BA.

> *An investigator must utilise knowledge of a character, if it is available, to understand how they might conceal any hidden truths. Character details is usually not available, so usually I would not be able to utilise BEA.*

A final interpretation was that participants might have thought that they did not utilise BA in their investigations; yet, they had performed or partially performed BA without direct awareness. Even though only 47.7% reported having knowledge of BEA, an average of 73.7% of the participants who have investigated SEIC reported utilising all of the six different activities that constitute BA when investigating SEIC cases either always or most of the time. Similarly, an average of 76.5% of the participants who had investigated cyberstalking cases reported utilising all of the different activities that constitute BA to either always or most of the time. This suggests that utilising BA is a process that comes naturally to skilled DF professionals. The benefits of utilising BA are apparent to most of the DF practitioners even though their knowledge of it is limited.

The majority of the participants believed that BA has the potential to contribute to many aspects of the investigation process. Most of the perceived benefits of BA during investigation of crimes that were solicited from participant's input were consistent with findings from previous research (Copson, 1995, Jackson et al., 1994, Pinizzotto, 1984, Snook et al., 2007, Trager and

Brewster, 2001). These benefits included shortening the time of investigation, reducing the suspect pool, providing insights on the motivation of the offender, and providing interrogation strategies. As earlier studies showed that BA has assisted in investigating cases that involved different types of traditional violent crimes. The results of this study, however, showed that the use of BA strategies has evolved to cover a wider range of criminal cases including cases that use technology to facilitate committing the criminal acts (e.g., SEIC and cyberstalking cases).

6.5 Summary

This study addressed the third objective of the programme of research, which was to examine the current use and perceived utility of BA in policing and law enforcement. Results showed that despite the high percentage of participants reported strong perceptions on the utility of BA in DF investigations, a considerable number of them hesitated when it came to its practical application. Possible interpretations and rationales for these findings were offered and discussed.

The study identified a number of challenges that limits the use and applicability of BA. Among them was the lack of proper knowledge and guidelines for applying BA in the digital forensics domain. This raises the need to include BA in training programs for DF practitioners. Conducting basic BA during the process of DF investigation of SEIC and cyberstalking crimes to at least understand patterns of the criminal behaviour, relationships between victims and offenders, and the sequence of crime events should be part of a thorough investigation. Even though SEIC and cyberstalking are technology-based crimes, the human element is still there. Traditional investigative technique must also be considered when investigating these crimes.

The next chapter combines the findings reported in this chapter, along with the findings in chapters 4 and 5 in an attempt to produce a usable model that integrates aspects of BA within the DF investigation process, and provides a structured guideline for its performance.

7 THE BEHAVIOURAL DIGITAL FORENSICS INVESTIGATION MODEL

7.1 Introduction

The previous chapters discussed the potential benefits of Behavioural Analysis (BA) in Digital Forensics (DF) investigations. However, based on results from surveying digital forensics practitioners (see Chapter 6), the daily practices of digital forensics investigations involve a very limited use of this technique. With the increased rate, complexity, and challenges of investigating digital crimes (Grispos et al., 2013, Oriwoh et al., 2013, Quick and Choo, 2014), it is important to integrate specific strategies of BA within the commonly used DF investigation framework. This study proposes a DF investigation model that incorporates aspects of BA. It aims to provide a pragmatic, structured, multidisciplinary approach to performing a post mortem examination, analysis, and interpretation of the content of the digital devices associated with computer-facilitated interpersonal crimes. The model adheres to commonly used DF process principles (i.e., confidentiality, integrity, and availability) (Ieong, 2006). The design of the model is based on empirical, practical testing of the investigative utility of BA on real Sexually Exploitative Imagery of Children (SEIC) and cyberstalking cases as described in Chapters 4 and 5.

This chapter addresses the final objective of the thesis, which is to integrate the findings of the preceding objectives into a usable DF investigation model that incorporates aspects of BA by identifying the phases and sub-phases required to perform the examination, analysis and interpretation of digital evidence for computer-facilitated interpersonal crimes. Two case studies

will be used to illustrate the investigative importance of the model in investigating computer-facilitated interpersonal crimes. They will demonstrate the value, as well as the limitation of the model.

7.2 Model Design

The proposed four-stage model was designed using a high-level categorisation in order to enable generalisation across different types of computer-facilitated interpersonal cases. It is presented in a linear format so as to provide a general and clear overview of the phases and sub-phases of the investigation. However, in practice, it is a dynamic and iterative process. New evidence about the victim, offender, and offending process can appear throughout the course of an investigation which raises new questions, and requires the re-investigation of previous stages (e.g., search for additional evidence or information, re-examination of specific data, reinterpretation of evidence).

The design of the model is based on empirical, practical testing of the investigative utility of BA on real SEIC and cyberstalking cases. The model's phases and sub-phases were also derived from Roger's behavioural analysis model (2015), and the DF profiling methodology for the cyberstalker proposed by Silde and Angelopoulou (2014) reviewed in Chapter 2. These models were selected because they encompass aspects of BA though not explicitly described.

The model has four phases: (1) review, (2) identification and collection, (3) examination and analysis, and (4) interpretation and reporting. The phases which involve BA are the *review phase* and the *examination and analysis phase*. The review phase has three BA-related sub-phases: context, classification, and prioritisation, while the examination and analysis phase consists of two BA-related sub-phases: content analysis and timeline analysis & mapping. Figure 7.1 shows a visual representation of the model with a breakdown of these two phases.

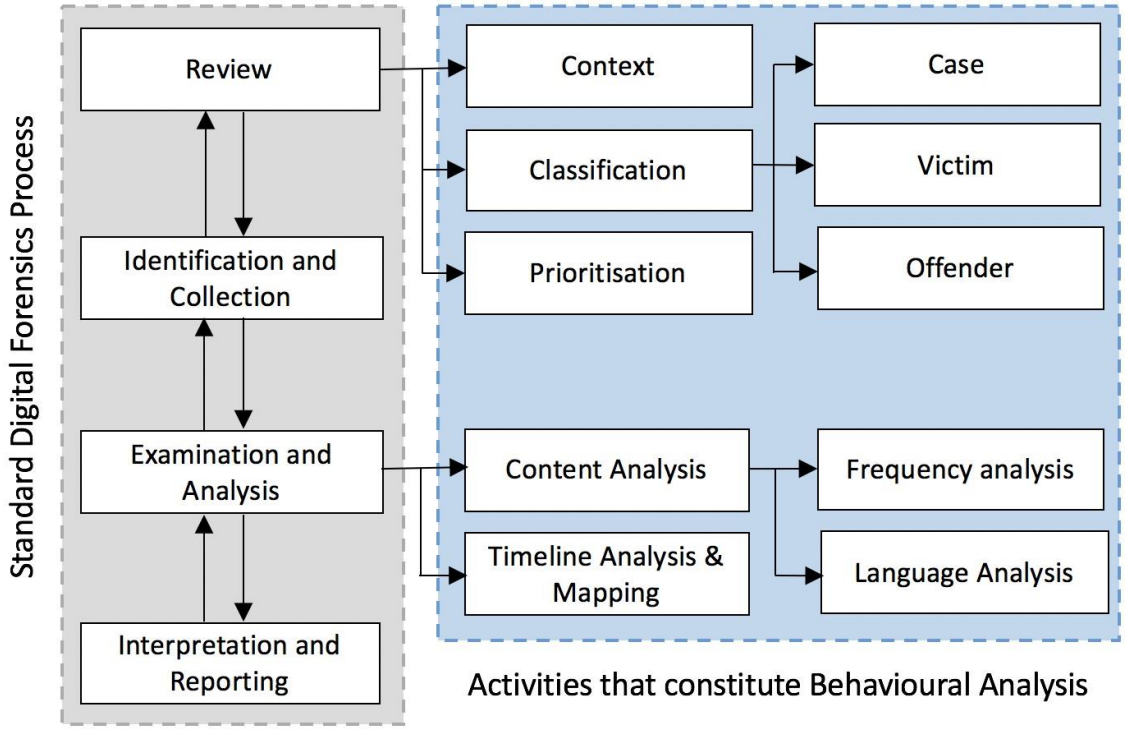


Figure 7.1 The Behavioural Digital Forensics Investigation Model

This section provides a discussion of the primary phases and the sub-phases of the proposed model, and describes the key tasks in each phase.

7.2.1 Phase 1: Review

The initial phase involves gathering as much information about the case to be investigated as possible. It helps the investigator to develop an initial overview of the case, and the involved parties. The outcome of this phase enables the investigator to prepare a strategy for the investigation (e.g., design a specific search criterion, form a specific hypothesis). Sub-phases are described in Sections 7.2.1.1-7.2.1.3.

7.2.1.1 Context

It is essential to understand the context of the case prior to examining and analysing the associated evidence. The investigator should perform a careful review of all the available case documents. This includes information about the case, related background and the people involved. Demographic details and descriptions of the suspect(s) and victim(s) (when known) must be noted (e.g., age, gender, ethnicity, employment status, marital status, qualification, and computer literacy). Other information about the offender' specific characteristics, including history of assaultive behaviour, criminal record, and psychiatric history, should also be identified and included. This can assist the investigator in determining the risk that the offender

poses (e.g., escalating from cyberstalking to physical stalking, or acting upon threats made). It also enables the investigator to determine the technical skill level of the offender and the possibility of facing anti-forensic techniques when examining and analysing the associated digital evidence.

Interview scripts with victims and offenders, and victim statements must also be reviewed. The investigator can compare this information to the results of the analysis of the digital evidence in the later stages of the investigation. This enables them to confirm or refute the offender or victim statements. All assumptions and interpretations from other investigators involved in investigating the case must also be considered. This enables the investigator to contextualise the case and develop an initial understanding of the events surrounding the incident. It also provides them with an initial profile of the offender which can inform the later stages of the investigation.

7.2.1.2 Classification

This stage consists of three types of classification: case classification, victim classification, and offender classification. After understanding the context of the case, the investigator can classify the category of the case and determine its initial level of complexity. Different types of cases (e.g., SEIC, cyberstalking, fraud, extortion) have unique characteristics and dynamics. Further, cases within the same crime category differ from one another in technical and behavioural aspects (e.g., level of complexity, technique, number of suspects, offender motivations). As such, classifying the case based on the available information enables the investigator to plan a strategy for the examination and analysis phase. This strategy is further informed by the *prioritisation* sub-phase discussed in Section 7.2.1.3.

Building a profile of the victim is also an important step in answering case questions. In addition to the victim's demographics, technical skills and physical characteristics, understanding their behavioural characteristics also brings benefits to the investigation. This enables the investigator to determine factors which provided opportunities for victimisation, and to identify the relationship between the victim and the offender. As such, understanding the victim is an initial step for understanding the offender and their motivations. In many cases, victim statements and interviews have gaps and loops, and do not provide a complete picture of the incident. Research suggests that full and accurate memory is difficult to achieve during police interviews due to cognitive limitations for victims or witnesses (Fisher et al., 1989, Geiselman and Fisher, 2014). It also suggests that poor interview strategies disrupt the natural process of memory retrieval (e.g., by interrupting the victim repeatedly during a narrative response). This include encouraging the victim to provide uncertain answers (e.g., repetitive questions that pressure the victim to provide answer for), preventing the victim from providing

detailed answers (e.g., asking closed-ended questions), and overloading the victim's limited cognitive capacity (e.g., asking too many questions) (Fisher et al., 1989, Fisher et al., 1987, Geiselman and Fisher, 2014, Vrij et al., 2014). In other cases, the victim might not provide a truthful account of the events that led to the incident. This was the case in a number of cyberstalking sample cases examined in Chapter 5, where the victim withheld information about their prior relationship (e.g., intimate relationship) with the offender. They also hid their role in initiating the events that led to the cyberstalking (e.g., ending the relationship). The investigator needs to use evidence gathered from the associated digital devices in order to fill in these gaps and develop a more detailed understanding of the incident. The investigators also need to weigh the conflicting and shifting stories about the incident in order to decipher what really happened. As such, the investigator can start by building an initial profile of the victim (based on information from the case documents), which can then be cross examined with results from the analysis of the associated digital evidence, to be updated at later stages of the investigation.

Classifying the offender is also an important step for planning a strategy for investigating the case. Based on the information collected in the *context* sub-phase, the investigator can construct an initial profile of the offender. This can include their demographic characteristics, technical skill level, and suspected motivations. Placing the offender within a specific typology can also be useful in certain categories of crimes (see sections 4.5.4 and 5.5.4).

At this point, the investigator should develop initial criteria for the relevant potential evidence to look for when examining the digital devices associated with the case.

7.2.1.3 Prioritisation

This sub-phase deals directly with the digital devices associated with the case. At this point, the investigator will perform a quick preview of the contents of the seized devices. The aim of this sub-phase is to provide an insight on which device(s) contain potentially relevant evidence in cases were more than one device were seized and brought to the lab for examination. It also provides insights which can enable the identification of the potential location of evidence on each device based on the criteria developed in the preceding sub-phases. This allows sorting of the devices accordingly in preparation for examination.

As time and data volume are two of the main constraining factors in DF investigations (Guarino, 2013, Lillis et al., 2016, Noblett et al., 2000), this sub-phase helps the investigator to prioritise the devices under investigation, determine a starting point for examination and analysis, and develop an examination plan (e.g., prioritise search goals). This can reduce the amount of time wasted in performing an unstructured examination of a huge number of potentially relevant files.

7.2.2 Phase 2: Identification and Collection

An essential step when starting the investigation of the digital devices seized is to identify the authorship of the evidence files and artefacts stored in them (Chaski, 2005, Rocha et al., 2017, Rogers, 2015). Unless it is ascertained that only a single individual had access to the device under investigation, the investigator must establish a verifiable link between the incriminating files and a potential suspect. A computer system can have more than one user profile, with each profile being accessed by a different individual. Furthermore, in some cases, a single profile is shared by more than one individual. The examiner must also consider the possibility that suspected offenders might be, in fact, victims themselves, and that their devices might have been accessed and misused by the real offenders (e.g., hacked and accessed remotely, real offender knows the password and has physical access to the device). Depending on the complexity of the case, the investigator might have to use a combination of techniques in order to identify and collect the required evidence files and artefacts (e.g., corroborate timestamps of the files with the suspect's real time use of the computer, check for viruses or software that enable remote access to the computer, conduct analysis of distinguishable language in written communications and online activities) (Chaski, 2005, Nirkhi and Dharaskar, 2013, Rashid et al., 2013, Rocha et al., 2017, Shavers, 2013). It is also worth noting that, in some cases, determining the author of the evidence files and artefacts can be very challenging (Shavers, 2013), or cannot be accomplished at all.

Once the investigator positively identifies evidence files, they should then be collected and sorted in a way that will enable the performance of focused, structured examination and analysis.

7.2.3 Phase 3: Examination and Analysis

This phase involves examining and analysing the collected data to produce information that can answer questions associated with investigating the case, and confirm or refute associated hypotheses. It consists of two sub-phases: content analysis and timeline analysis, described in Sections 7.2.3.1 and 7.2.3.2.

7.2.3.1 Content Analysis

In digital interpersonal crimes, many of the digital files and artefacts on a subject's digital device reflect the behaviour of the person who created those files (i.e., the suspect or the victim). A careful examination and analysis of those files can help the practitioner to identify evidence that can be attributed to a specific suspect, understand the relationship between an identified suspect and a victim, identify the predominant motivation of the offender, and understand the context in which the incident occurred. As such, this sub-phase involves

performing qualitative and quantitative analysis of the material stored within the digital files and artefacts. Two types of content analysis can specially bring benefits to the investigation of digital crimes: frequency analysis and language analysis.

As most computer-facilitated interpersonal crimes involve the online activities of suspects and victims, it is essential to analyse the different behaviours that are reflected by these activities. For example, in SEIC cases a frequency analysis of the visited websites, downloaded files, search history, and cache files can provide various investigative leads. It can also help the practitioner identify the periods of high online activities and/or computer usage, mostly visited websites, and the mostly downloaded or traded files (Rogers, 2015, Rogers and Seigfried-Spellar, 2014). Referring to the SEIC evidence interpretation table in chapter 4 (see Table 4.4), the volume of SEIC on the suspect's computer, plus the frequency of SEIC-related search queries and the frequency of related visited websites can be of significant investigative utility. These factors can provide sufficient evidence that the user intentionally sought out SEIC and exercised control over them.

Language analysis involves examining and analysing contents of written communications (e.g., emails, chat logs, text messages). As most interpersonal crimes involve written communication between suspects and victims, this information can be invaluable to the investigation. For example, cyberstalker quotes illustrated in Table 5.5 in chapter 5 demonstrated that many cyberstalkers express (through written communication) their inner emotions (e.g., rage, love) that led them to cyberstalk their victims. This can provide the practitioner with an indication of the motivation behind the offender's behaviour. Using a specific writing style and vocabulary can be significant psychological indicators of the emotional state of the offender (Hancock et al., 2013). It can also reflect offenders' motivations and the potential risk they pose to the victim. In cases of multiple suspects, the writing style and language can be distinctive enough to differentiate between them. Repetition of certain errors and the frequent use of specific words or phrases can be linked to a specific suspect. Language analysis can also reflect the traits and behaviour that contributed to the victim being targeted by the offender. A treatise on language analysis in assisting digital investigations is beyond the scope of this work, however, an example of a comprehensive work on this subject was performed by Shaw (2006).

Since each case has its unique set of characteristics and details, it is essential for the practitioner to customise the content analysis undertaken in accordance with the specific characteristics of the case.

7.2.3.2 Timeline Analysis & Mapping

This sub-phase involves analysing time stamps associated with the files in question and cross examining them with the time frame in which the crime events occurred Rogers (2015). An

essential step after collecting the related digital evidence is to make sense of them by organising them chronologically. Whenever possible, the investigator must examine the date and time-based information associated with the evidence files and map them onto other timestamps collected in the previous phases (e.g., from background story, victim interview). Files can be sorted, grouped, or filtered to generate a representative dataset that aids in the interpretation and reconstruction of the events of the crime. Such a dataset can also provide a better overview of the activities involving the suspect and victim, and reduce confusion in understanding the order of the events. It can also provide a timeframe of activities that can confirm or refute the claims of the victim/offender. In cases where more than one suspect had access to the same user account, producing a timeframe of user activity combined with other forms of content analysis which can be compared to users' real time activities can be used to eliminate suspects, and determine the probable offender (Rogers, 2015). Analysing the variation in a file's timestamp (i.e., created, accessed, modified) can indicate users' behaviour towards the file, and whether they had misused it. For example, timestamp of file creation precedes timestamp of modification can indicate the user had altered the file. As such, in many cases timestamp analysis will be a significant part of the investigation.

7.2.4 Phase 4: Interpretation and Reporting

In the final stage of the investigation, the practitioner attempts to define and contextualise all the events that took place during the course of the crime in order to answer the associated investigative questions. At this stage, it is especially important for the practitioners to stay objective and consider all the different possibilities and interpretations of the combined analysed evidence and timeframes. They would establish the timeline of events and attempt to reconstruct the crime based on the evidence collected and analysed during the previous phases. This would then be used to build the report to the requesting party.

Section 4.4 in chapter 4 and section 5.4 in chapter 5 provided interpretation tables that can aid investigators in interpreting specific evidence related to SEIC and cyberstalking cases. They can also assist in establishing the significance of the processed digital evidence, and help the investigator to form hypotheses about the suspect's actions. This can enable a more detailed reconstruction of evidence that can inform sentencing and prosecution.

7.3 Limitations

Whilst the proposed model provides a useful tool for the investigation of certain types of computer-facilitated interpersonal crimes, it is important to recognise that it is not without limitations. The use of the model is affected and is limited by the availability of sufficient case information, and the availability of a significant amount of digital evidence. The accuracy and

detail of the analysis is also limited by the accuracy and detail of the evidence on which it is based. For example, a poorly described case background can result in the practitioner gathering very little reliable information during the *Review* phase (for the context, classification, and prioritisation stages). Having a weak base of reliable case information can affect the later phases of the model as well (i.e., Identification and Collection, Examination and Analysis, and Interpretation and Reporting) resulting in a misguided, unfocussed investigation. On the other hand, the BA introduced within the model will be of greater utility when there is a variety of digital evidence that can be used to infer the actions of the offenders/victims (such as, written communications, Internet history files). For example, the use of anti-forensics techniques by the suspect to eliminate traces of their online activities and communication with the victim can prevent a considerable amount of important data being analysed behaviourally. This would limit the utility and benefits of using the model.

Another major limitation is finding an individual who is competent in both DF and BA. To get the most benefit from the model, it is essential for the practitioner to be well equipped with skills in both disciplines and have enough knowledge in both areas. The practitioner's critical skills, intuition, and judgment can have a high impact on the application and outcomes of the model. The practitioner must utilise all the previous skills and work with caution and objectivity to provide the most appropriate analysis and interpretations of the recovered digital evidence. This indicates the importance of training in the relevant disciplines. However, there is always the possibility of unintentionally including the practitioner's subjectivity and bias in interpretations. It is also important for the practitioner to acknowledge the dynamic and flexible nature of the model and utilise it accordingly. The practitioner should have the ability to customise the model to the specifics and different attributes of the case under investigation. Following the model steps literarily without considering the unique aspects of each case can greatly limit its investigative value.

The previous limitation, however, can be addressed by working in multidisciplinary teams, especially for complex cases. Such cases would benefit from the technical skills of a DF investigator and the analytical skills of a behavioural analyst working closely together on the investigation of the digital evidence

7.4 Case Studies

This section elaborates on two case studies related to computer-facilitated interpersonal crimes. These cases illustrate the application and utility of the model depicted in Figure 7.1 for the DF processing of evidence. The criteria used for selection of cases are also described in Chapter 3.

It is important to note that the researchers did not review the original report that included the results of examination and analysis of the cases prior to conducting the DF investigation. This was to ensure that the investigation process using the model was not influenced or guided by the original results from the case documents. As such, the original results were only reviewed *after* the researcher concluded the case analysis in order to compare the findings. Sections 7.4.1 and 7.4.2 elaborates on the use of the proposed model.

7.4.1 Impersonation and Defamation on Facebook

The case involves three types of criminal conduct: (1) theft of user login credentials, (2) online impersonation of a user through Facebook, and (3) harassment via online defamation and slander. A female (Miss X) filed a complaint at a local police station that she had been impersonated and defamed through her Facebook account. She stated that her account was hacked and used to post offensive information on her profile page (Facebook/Education and Work section) during the month of July 2010. She did not suspect anyone in particular. Initial investigation conducted by the Cyber Police Section at the Criminal Investigation Department (CID), of which the details were not provided in the case documents, traced the origin of the activity to an Internet account that belonged to a male suspect (Mr Y). Mr Y was requested to attend for interrogation. During the interview, Mr Y denied the accusations and claimed not to have any previous knowledge of Miss X. A search warrant was issued to search Mr Y's residence where three laptops were seized for post-mortem examination. Two of the laptops had a sticker with "Mr Y" handwritten on them, while the third had the name of Mr Y's spouse on it. The case request letter asked to examine the seized laptops to identify whether they had been used to login to Miss X's Facebook account and post the defamatory information.

It is important to note that all of the case documents, interview scripts, and the posted defamatory information were in Arabic. Information necessary for the case study was translated into English by the researcher. Also, to conceal the identities of the involved parties, pseudonyms have been used for the victim, suspect, spouse of the suspect, and locations. The researcher has obscured profanity throughout this section. The remaining of this section provides a walk-through of the investigation using the proposed model.

7.4.1.1 Phase 1: Review

As illustrated in the DF Behavioural Model (see Figure 7.1), the first phase has three BA-related sub-phases: context, classification, and prioritisation.

7.4.1.1.1 Context

This sub-phase involves a careful study of all the related case documents. The researcher collected information on the victim (Miss X), suspect (Mr Y), and the offence. Miss X'

statements and interview scripts revealed a number of interesting pieces of information. She was a single woman from the Middle East, aged 32, who lived in an apartment with a (female) roommate. She worked in a private sector company and shared an office with two other individuals (also females). Her working hours were from 9:00am to 5:00pm. She had been working in the company for 3 years and was recently promoted to a higher position. When asked if she used her office workstation to access her personal accounts, her answer was positive. She used to check her personal email and Facebook accounts during her lunch break. Her workstation was password protected, yet, she admitted that she would sometimes leave it unlocked if she needed to leave the office for a short time (without specifying the exact length of time). She also stated that there were a number of instances where her office colleagues have used her workstation through her user account. According to her, she did not have any reason to suspect any specific individual. Miss X said that she shared a single laptop with her roommate using the same user account. Further, she claimed not to have previous knowledge of the male suspect (Mr Y) identified so far.

The case documents provided little information about Mr Y. In his interview script, Mr Y claimed not to have any involvement in the incident. He was a 39 years old male who worked in a different private sector company to that of Miss X. He lived with his spouse in an apartment, and had no children. Both he and his spouse had their own laptops and did not share or use each other's devices. He claimed not to have any previous knowledge of Miss X, nor her Facebook and email accounts. The case documents also included information related to Miss X's office colleagues and roommate, which was gathered during the initial investigation by the CID. This included their names and details of their email accounts.

The case documents included the email account that Miss X used to access her Facebook account, and a copy of her Facebook page that was altered and used to post the defamatory information. Figure 7.2 shows the Facebook page in question. Note that all identifying information was blurred by the researcher to preserve Miss X's anonymity.

Figure 7.2 Defamed Facebook page of Miss X.

The copy of the altered Facebook page was examined and all information that was thought to be relevant to the investigation was noted (e.g., Facebook profile ID, defamed Miss X's name on the page, defamatory information). Miss X's original profile name was altered to *Miss X the Frog*. The defamatory information published on the Education and Work section was:

Employers	*Houses of prostitution and nightclubs in (X City).*
College	*(Country X) country of prostitution and wh@$ing.*
High School	*School of bit@$ing and wh@$ing.*

7.4.1.1.2 Classification

Initially, the incident was categorised as an interpersonal offence that constituted at three types of criminal conduct (see beginning of Section 7.4.1). The fact that three individuals (Miss X's roommate, and her two work colleagues) were usually within close range to Miss X, and had physical access to computers belonging to her, led to the presumption that the MO of stealing her user login credentials could have been performed with relative ease. Based on the possibility, it has hypothesised that one of them was involved in the offence. As such, after gaining access to Miss X's Facebook account, impersonation and publication of the defamatory

information could have been performed with minimum difficulty. This was unless measures were taken by the offender to hide the evidence of their criminal activity.

The daily activities of Miss X had created opportunities for victimisation. For example, she had been logging into her personal accounts using her office workstation. If she was, for example, targeted by an individual working in the Network Department, it would have been relatively easy to intercept her network traffic and steal her login credentials. Leaving her workstation unlocked, even for few minutes, would also put her at risk of victimisation. A few minutes is enough time to install a keylogger or monitoring software on a computer. Sharing her computer with others also increased the potential of being victimised. The following are quotes from her interview script that have been transcribed into English. The quotes show some of Miss X's activities that might have increased her risk of victimisation:

> *I check my Facebook and my personal email every day, usually during my break time.*
>
> *I use my office workstation to check my personal email and Facebook.*
>
> *Yes, I do leave the office sometimes without locking my workstation, but it's usually for a few minutes, when I go to the washing room, or go grab a cup of coffee.*
>
> *My office colleagues used my workstation a number of times. I was in the office at the time though.*
>
> *My relation with my office colleagues is only through work. It's not like we are friends.*
>
> *My roommate and I share the same laptop, same user account. We are close friends.*

The case documents and interview scripts did not provide enough information to predict a motivation for the initial suspect (Mr Y). However, one possible motivation could have been a prior, but undisclosed, relationship between Mr Y and Miss X that neither were admitting. No further assumptions could be made about Mr Y before an initial examination was performed on the seized laptops.

The information collected at this phase enabled the generation of three hypotheses in relation to who could have committed the offence: (1) Mr Y, (2) one of Miss X's office colleagues, or (3) Miss X's roommate. The first hypothesis was based on the fact that the investigation conducted by the CID had identified Mr Y as an initial suspect. It was also based on the possibility of Mr

Y not being totally truthful in his interview statements in relation to his involvement in the offence, and his knowledge of Miss X. The second hypothesis was that one of Miss X's office colleagues was linked to the incident. This was based on the fact that they had accessed her workstation a number of times, which provided a means to steal her Facebook credentials (e.g., observed Miss X while typing the password, used a keylogger). One possible motivation in this case was jealousy or anger associated with Miss X's promotion. The third hypothesis was that Miss X's roommate was involved in the incident based on the fact that they shared the same computer and user account. However, there was not enough information to suggest a possible motivation for her involvement.

Despite forming the previous hypotheses, other possibilities were also considered (e.g., the spouse of Mr Y being involved in the incident, Miss X herself trying to incriminate someone). However, the data available at this stage lacked information that supported the formation of these last two hypotheses. Confirming or refuting the generated hypotheses would require analysis of the evidence from the seized digital devices. The generation of new hypotheses was based on the next stages of the investigation.

7.4.1.1.3 Prioritisation

In order to prioritise the laptops seized, a quick string search was performed on specific locations on each laptop that were more likely to contain evidence related to the incident (e.g., Internet history folders, Unallocated Clusters). Unique words and phrases on Miss X's defamed Facebook page (see Figure 7.2) were used to perform the search (e.g., Miss X's Facebook profile ID number, email ID, defamed name of Miss X). A decision was made to begin the examination and analysis with the laptop that started showing positive search hits. Interestingly, and unexpectedly, positive hits started to appear on the laptop belonging to the spouse of Mr Y (Mrs Y).

7.4.1.2 Phase 2: Identification and Collection

This phase started by identifying user accounts on the laptop. There was one user account, which was password-protected and had the same name as Mrs Y. Performing a full string search resulted in 349 hits on Miss X's email account, 407 hits on Miss X's Facebook ID number, and 385 hits on Miss X's name. The first round of string searches, however, resulted in zero hits on the defamatory phrases published on Miss X's Facebook page. The characters of Arabic phrases were converted into Unicode escape characters, and a second search session was run using the equivalent set of Unicode (Al Mutawa et al., 2011). The search session resulted in 3 and 4 hits on two of the insulting phrases posted on Miss X's Facebook page. All the files that contained the search hits were selected and sorted to be further examined and analysed.

7.4.1.3 Phase 3: Examination and Analysis

As illustrated in the DF Behavioural Model (see Figure 7.1), this phase has two BA-related sub-phases: content analysis, and timeline analysis and mapping. Sections 7.4.1.3.1 and 7.4.1.3.2 describes how these sub-phases were conducted in investigating the sample case.

7.4.1.3.1 Content Analysis

Results showed that the majority of the search hits on Miss X's Facebook profile ID were in a specific index.dat file (i.e., a database file used by the Internet Explorer web browser to store information on user Internet activity such as visited web URLs, and timestamps of access). The specific index.dat file that included the hits was stored in the location: ..\Users\(Mrs Y)\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat. The file was extracted and the Index.dat Analyzer software was used to further analyse its contents. The file contained 1329 entries from which 376 were associated with Miss X's Facebook page. Entries showed that the user had logged into the Facebook account of Miss X and visited pages that enabled editing its contents (e.g., Miss X's profile and album). The entries also showed that the user had entered the editing page for the Education and Work (i.e., the page that was defamed).

The other search hits were within fragments of source code found in the Unallocated Clusters. Analysing parts of the source code also showed that the user had logged into the Facebook account of Miss X and visited pages that enabled editing its contents (e.g., Miss X's profile and album). Likewise, the entries showed that the user had entered the editing page for the Education and Work (i.e., the page that was defamed). Further examination of the contents did not show evidence of hacking software, keyloggers, or software that enables remote monitoring.

The final step consisted of running a search on the email accounts of Miss X's office colleagues and roommate to find if they had any connection with the user. Results showed 132 hits on the email account of one of Miss X's office colleagues. Analysing the contents of the available emails showed a relationship between the user and Miss X's office colleague, which could be described as friendship. It included casual style correspondence mainly covering everyday activities. Some of the emails contained e-cards, as well as entertaining jokes and pictures. The contents of the emails exchanged during the two months period prior to the incident showed a considerable amount of negative comments from Miss X's work colleague aimed towards her body weight and her work. It indicated on the state of mind and feelings of Miss X's work colleague during that period of time (e.g., anger, frustration, envy). The following are quotes that have been extracted from Miss X's work colleague emails and transcribed into English:

> *I am so short of time, I want to exercise at home, but I don't know.. everything is just not working. It infuriates me to see my body this way. It makes me eat more and do not exercise.*
>
> *Now I am moving from one nutritionist to another. I have to close my mouth but I cannot.*
>
> *My schedule is sh@t. Many things are happening at work. I try to take it easy, but it is still affecting me.*
>
> *I am fed up tolerating with all the stupid sh@t-heads at work.*
>
> *I am losing my talent in presenting my work. I do not want them to think that I am useless.*
>
> *It is very unfair. The stupid bit@$es get promoted, while I'm rotting on my seat for almost 5 years now!!.*

Performing a full string search on the two laptops belonging to Mr Y did not result in any hits.

7.4.1.3.2 Timeline analysis & Mapping

Analysis of the timestamps associated with the entries identified in the previous section showed that the user had visited these webpages during the period 6–20/July/2010. It also showed that the peak time of activity was roughly between 11:30pm and 1:30am. This timeframe mapped with the information that Miss X provided in her statement, which is further elaborated on in the next section.

7.4.1.4 Phase 4: Interpretation

After analysis of the collected data, all the possible interpretations of the results were identified. The user online behaviour and the intense activity on Miss X's Facebook account during the period 6–20/July/2010 were consistent with the statements made by Miss X:

> *It happened (the defamation offence) sometime during the month of July. I tried to log into my account several times but couldn't. That's when I realised that it was compromised. Then I saw the published information on my page.*

As the analysis confirmed, the user had been logging into Miss X's Facebook account, and visiting different pages in her profile. It also showed that the user had performed editing actions on the Work and Education page, yet no evidence was found of the specific changes that had been performed.

Combined with Mr Y's claims of not having any knowledge of Miss X or the offence, and not finding any evidence on his laptops, there was a strong indication that Mrs Y was the individual behind the incident. A question that then arises is how and why was Mrs Y involved in the offence? A statement made by Miss X claimed having no previous relation or knowledge of Mrs Y:

> *I do not know Mr Y, nor do I know Mrs Y. I do not have any previous relation or knowledge of them.*

The correspondence found between Mrs Y and the Miss X's office colleague indicated the possibility of a second suspect (i.e., Miss X's work colleague). The quotes listed above showed that Miss X's work colleague had a level of dissatisfaction and negative issues about her body weight and her work. The last quote was indicative of her feeling disgruntled for the promotion of other employees, even though it did not contain any explicit statements related to the incident or the victim:

> *It is very unfair. The stupid bit@$es get promoted, while I'm rotting on my seat for almost 5 years now!!*

The interpretation of all the extracted evidence resulted in:

1. Refuting the first hypothesis suggesting that Mr Y was the suspect.
2. Refuting the hypothesis that Miss X's roommate was involved in the offence.
3. Providing supporting evidence to the hypothesis that one of Miss X's office colleagues was involved in the offence.
4. Providing evidence that supported the generation of a new hypothesis suggesting that Mrs Y was involved in the offence.
5. Providing evidence suggesting that Mrs Y and Miss X's office colleague were co-conspirators, with a possible motivation of Miss X's colleague being disgruntled and taking out her rage on Miss X. Since they were "friends", Miss X's office colleague might have provided Mrs Y with Miss X's Facebook login credentials and convinced her perform the misconduct.

Results from this stage would have directed the main researcher to request performing further investigations to support or refute the newly generated hypothesis. This would consist of: (1) interrogating Mrs Y and Miss X's office colleague based on the evidence found to correlate what was found to their statements, (2) examining Miss X's workstation for a possibility of gathering evidence of the MO of stealing her Facebook login credentials. However, the case was an archived file. Therefore, the researcher had to use what was available and no further

investigation was possible. As such, confirming or refuting the newly generated hypotheses was not possible and the investigation had to be ceased at this point.

7.4.2 Employment and Money-Forwarding Scam

The following case involves four types of criminal conduct: (1) online fraud, (2) money laundering, (3) using a fictitious identity online, and (4) hacking. On the 31st/Dec/2012 a request letter arrived from a local police station. The letter stated that a British female (Ms A) had filed a complaint on the 5th/Aug/2012 stating that on the 21st/Jun/2012 she logged into her online HSBC bank account to find that someone had hacked into it and performed three money transfers with a total sum of 154,849 UAE Dirhams (approximately 31,671 British Pound Sterling, and 42,164 US Dollars). The funds were transferred to the bank account number xxx-xxxxxx-xxx belonging to a male of a Zimbabwean nationality (Mr R).

Mr R was requested to attend for interrogation. During the interview, he claimed not to have any previous knowledge of Ms A. He claimed that he had received the funds in his bank account (xxx-xxxxxx-xxx) during the month of June 2012. He also claimed that earlier the same month his wife (Mrs R) had signed an employment contract with a company based in South Korea, which claimed to be opening a branch in Dubai soon. According to Mr R, the company requested that his wife provide her personal bank account details so that they could transfer the funds required to establish the new branch in Dubai. Since Mrs R did not have a personal bank account, she provided them with Mr R's bank account details (xxx-xxxxxx-xxx). The company had then transferred some funds to the provided bank account and asked Mrs R to withdraw the cash and resend it to a third party (as part of the company) through a money exchange service.

A search warrant was issued to search Mr R's residence where three laptops were seized for post-mortem examination. The laptops did not bear any stickers to show which belonged to Mr R or Mrs R. The case request letter asked to examine the seized laptops to identify "relevant evidence".

All of the case documents, and interview scripts were in Arabic. Information necessary for the case study was translated into English by the researcher. However, all of the evidence extracted from the laptops was in English. Also, to conceal the identities of the involved parties, pseudonyms have been used for the victim(s), and suspect(s). All identifying information has also been removed (e.g., bank account numbers, mobile phone numbers, personal email accounts). The remaining of this section provides a walk-through of the investigation using the proposed model.

7.4.2.1 Phase 1: Review

As illustrated in the DF Behavioural Model (see Figure 7.1), the first phase has three BA-related sub-phases: context, classification, and prioritisation.

7.4.2.1.1 Context

The first phase of the analysis consisted of conducting a careful examination of all the related case documents. The researcher collected information about the victim (Ms A), the suspect (Mr R), and the offence. Very little information was available about the victim (Ms A) as the only details available were her statement when she made the complaint (see Section 7.4.2), and her bank account number (yyy-yyyyyy-yyy). The case documents did not include any interview script with Ms A. As such, what is known about Ms A was that her HSBC bank account was compromised and three fund transfers were made during Jun/2012 to the account number (xxx-xxxxxx-xxx) belonging to Mr R. The exact amount of each transfer was not provided, however, the total sum of the three transfers were 154,849 UAE Dirhams.

Mr R's statement and interview scripts provided a number of interesting pieces of information. He was aged 45, from Zimbabwe, and currently living in Ras Al Khaima with his wife (Mrs R), aged 42, also from Zimbabwe. Mr R claimed not to have any knowledge or relation with the victim (Ms A). Nor was he aware that the funds transferred to his account were stolen from Ms A. He stated that his wife (Mrs R) had been between jobs for quite a while. She had been offered a part-time job from a company based in Korea (the company's name was not provided) that asked her to work as their representative in Dubai. She signed the contract with them in early June 2012. According to his statement, the company was going to open a branch in Dubai and requested that Mrs R process the company's funds needed to establish the new branch. As part of the requirements to take the job, Mrs R had to provide the company with her personal bank account number. According to Mr R, the company claimed that they were going to transfer funds to her account. Mrs R was to withdraw the funds and wire transfer them to a third party representative of the company. The bank account number that Mrs R provided the company was xxx-xxxxxx-xxx, which belonged to Mr R. Mr R also claimed that Mrs R had made the money transfers through two money services: Al Ansari and Emirates Exchange.

The case documents were limited to the previous information, and it did not include any interview scripts with Mrs R. As such, it was assumed that no interview was conducted with Mrs R.

7.4.2.1.2 Classification

Initially, the incident was categorised as an online financial fraud against an individual(s) that possibly constituted four types of criminal conduct: (1) hacking, (2) online fraud, (3) using fictitious identity online (the company), and (4) money laundering.

Ms A's statement that money was transferred from her online banking account led to the assumption that the offender had compromised/hacked her account. However, there was not enough information in the case documents to help establish a possible MO. Very little information was provided about Ms A, and there was no interview script. No details were provided about her daily online routines, or frequently visited websites, which could have been used to identify behaviour which might have placed her at risk of victimisation. Also, her computer/laptop was not brought for examination. As a result, it was concluded that the MO of compromising Ms A's online bank account, and factors that placed her at victimisation, could not be identified using the information provided in the case files.

The case documents and interview scripts did not provide enough information to predict a motivation for the initial suspect (Mr R). The story provided by Mr R sounded as if his wife (Mrs R) was a victim to an employment and money forwarding/processing fraud scheme. It seemed that Mrs R had been tricked into an online fraud scheme that used her to launder stolen money. However, this initial classification was based on the information provided in the case documents. It had to be reviewed and refined later once the seized laptops were examined and evidence extracted.

The information collected up to this point enabled the generation of a number of hypotheses in relation to the suspect(s) committing the offence:

1. The case at hand was part of a larger fraud scheme which involved other offenders. Ms A's online bank account was compromised by someone who is currently unknown. Her money was transferred by this unknown offender to Mr R's bank account.
2. Mr R was telling a true story about the online fraud scheme that tricked his wife into being a money mule for illegally acquired funds.
3. Mr R was not totally truthful, and he was part of the fraud scheme.
4. Mrs R was part of the fraud scheme.

A logical motivation for involvement in this type of fraud would be financial gain. Despite forming the previous hypotheses, the examination and analysis of the laptops was not totally guided by them. The examination should be open to other possibilities which can lead to the formation of new hypotheses. Confirming or refuting the generated hypotheses was based on the evidence analysed from the seized laptops.

7.4.2.1.3 Prioritisation

In order to prioritise the laptops under investigation, a quick string search was performed on specific locations on each laptop that were most likely to contain evidence related to the incident (e.g., Internet history folders, user created files and folders). Since the case documents did not provide much detail about the incident, the only unique strings that could be used were the bank account number of Ms A, her name, and the bank account number of Mr R. A decision was made to begin the examination and analysis with the laptop that started indicated positive search hits. When the search resulted in zero hits, another round of full search was performed. Halfway through the search session the first computer started showing hits on Mr R's bank account number. When the search sessions ended, the first laptop had 8 hits on Mr R's bank account number. The other two laptops did not show in any positive hits. The search hits on the first laptop were on the directory:

C\Users\Sony_vaio\AppData\Local\Microsoft\Outlook\

In a second attempt to prioritise the laptops, a quick manual search was performed on specific locations on each laptop (e.g., use created files and documents). Specific types of files which were thought might hold evidence related to the case were targeted (e.g., PDF, Doc, Docx, Microsoft Outlook Msg files, Internet history files). The second laptop showed two interesting folders which held a number of files with names that seemed to have some relation to the case. The following are a sample of some of the files and their paths:

1. C\My Documents\Personal\Case\Copies of transfer slips.pdf
2. C\My Documents\Personal\Mrs R- Employment\FW Part time Job Offer in U.A.E EMPLOYMENTCONTRACT-AGREEMENT.msg
3. C\My Documents\Personal\Mrs R- Employment\Mrs R- Employment Contract.pdf

An examination of the files indicated information that seemed to be related to Mr R's statements from his interview script. A decision was made to start the examination and analysis with this laptop. Note that no information was provided in the case files about whom each laptop belonged to.

7.4.2.2 Phase 2: Identification and Collection

This phase started by identifying user accounts on the second laptop as suggested by the previous stage of the analysis. The laptop did not have an identifying user login name, and it was not password-protected. However, the first folder of interest that was examined included the name of Mrs R (Mrs R- Employment). The directory which held the folder was:

C\My Documents\Personal\Mrs R- Employment

The folder held 4 files:

1. FileDownloadServlet.pdf
2. FW Part time Job Offer in U.A.E EMPLOYMENTCONTRACT-AGREEMENT.msg
3. Mrs R- Employment Contract.pdf
4. SMS.docx

The second directory of interest was:

C\My Documents\Personal\Case

It held a single pdf file: Copies of transfer slips.pdf

All the previous files were extracted for examination and analysis.

The first laptop did not have an identifying user name, nor was it protected by a password. The emails that had the 4 search hits in the folder C\Users\Sony_vaio\AppData\Local\Microsoft\Outlook\ were extracted. Also, a review of the titles of the emails sent and received during the month of June 2012 showed a number of possibly related emails (e.g., COMPANY APPLICATION FORM, Fw Part time Job Offer in U.A.E. EMPLOYMENT CONTRACT-AGREEMENT). All of these files were extracted for examination and analysis.

The third laptop also did not have an identifying user name or password protection. A full string search on all the possible case-related terms resulted in zero hits. A manual review of the directories did not reveal any possible case related evidence.

7.4.2.3 Phase 3: Examination and Analysis

As illustrated in the DF Behavioural Model (see Figure 7.1), this phase has two BA-related sub-phases: content analysis, and timeline analysis and mapping. Both sub-phases were conducted simultaneously when investigating the sample case. However, the researcher attempts to clarify how each sub-phase was conducted by describing them into two separate sections: 7.4.2.3.1 and 7.4.2.3.2.

7.4.2.3.1 Content Analysis

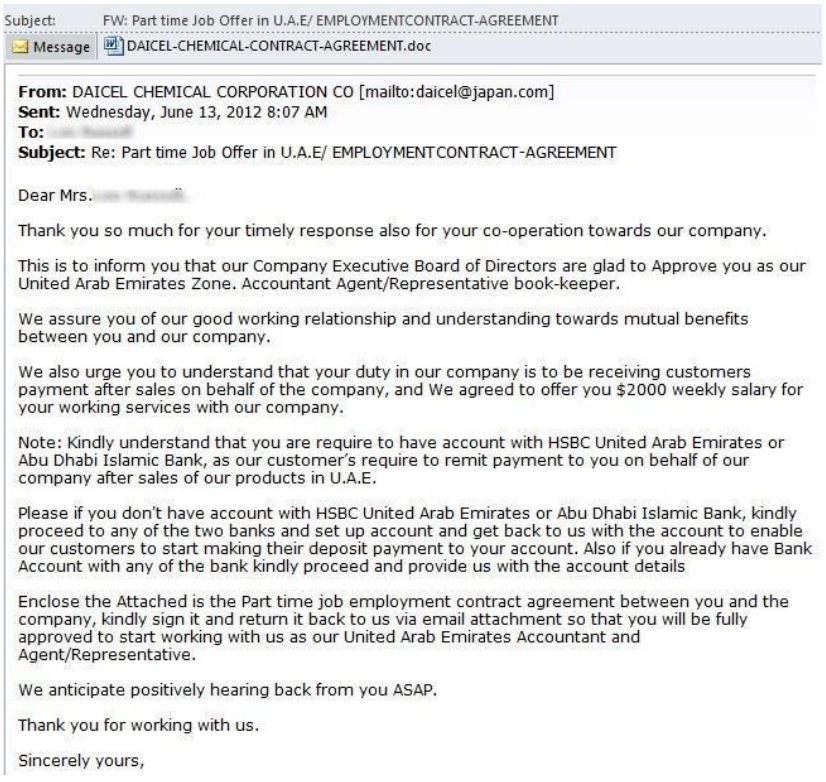
Analysing the contents of the files extracted from the second laptop showed the following:

1. The file "FileDownloadServlet.pdf" was an HSBC bank statement for Mr R's account (xxx-xxxxxx-xxx) which showed transactions performed between 16-21 of June 2012. The statement showed three deposits made from a Ms A as follows:
    a. On 14/Jun/2012 a deposit of 98,949 UAE Dirhams.

b. On 16/Jun/2012 a deposit of 55,120 UAE Dirhams.
c. On 18/Jun/2012 a deposit of 780 UAE Dirhams.

Summing the three amounts showed a total of 154,849 UAE Dirhams.

2. The file "FW Part time Job Offer in U.A.E EMPLOYMENTCONTRACT-AGREEMENT.msg" contained email correspondence (Figure 7.3) between a Mrs R and a company (DAICEL CHEMICAL CORPORATION CO) that used the email (daicel@japan.com). The email was forwarded between two of Mrs R's email addresses. The original email was sent from the company's email address (daicel@japan.com) and addressed to Mrs R. It was dated 13/Jun/2012 and stated that the company had agreed to have Mrs R as their Agent/Representative book-keeper in their United Arab Emirates Zone with a weekly salary of $2000. The company explained that Mrs R's duty would be to receive customer payments after sales on the behalf of the company. She was urged to provide the company with either an HSBC or Abu Dhabi Islamic Bank account.



Subject: FW: Part time Job Offer in U.A.E/ EMPLOYMENTCONTRACT-AGREEMENT

Message | DAICEL-CHEMICAL-CONTRACT-AGREEMENT.doc

From: DAICEL CHEMICAL CORPORATION CO [mailto:daicel@japan.com]
Sent: Wednesday, June 13, 2012 8:07 AM
To:
Subject: Re: Part time Job Offer in U.A.E/ EMPLOYMENTCONTRACT-AGREEMENT

Dear Mrs.

Thank you so much for your timely response also for your co-operation towards our company.

This is to inform you that our Company Executive Board of Directors are glad to Approve you as our United Arab Emirates Zone. Accountant Agent/Representative book-keeper.

We assure you of our good working relationship and understanding towards mutual benefits between you and our company.

We also urge you to understand that your duty in our company is to be receiving customers payment after sales on behalf of the company, and We agreed to offer you $2000 weekly salary for your working services with our company.

Note: Kindly understand that you are require to have account with HSBC United Arab Emirates or Abu Dhabi Islamic Bank, as our customer's require to remit payment to you on behalf of our company after sales of our products in U.A.E.

Please if you don't have account with HSBC United Arab Emirates or Abu Dhabi Islamic Bank, kindly proceed to any of the two banks and set up account and get back to us with the account to enable our customers to start making their deposit payment to your account. Also if you already have Bank Account with any of the bank kindly proceed and provide us with the account details

Enclose the Attached is the Part time job employment contract agreement between you and the company, kindly sign it and return it back to us via email attachment so that you will be fully approved to start working with us as our United Arab Emirates Accountant and Agent/Representative.

We anticipate positively hearing back from you ASAP.

Thank you for working with us.

Sincerely yours,

Figure 7.3 Employment letter agreement to Mrs R.

An employment contract agreement was also attached to the email, which she was asked to sign and send back to the company. A quote from the contract stated:

That the employee receives deposit payment funds on behalf of Daicel Chemical Corporation Co., Ltd whatever sum is found in his possession in favor of the employer and will be notified on how to remit the funds back to Daicel Chemical Corporation Co., Ltd when ever company require to remit the funds under your care.

3. The file "Mrs R- Employment Contract.pdf" constituted a scanned document of the contract agreement between the employee and Daicel Chemical Corporation Co., Ltd. It was signed, and the date "13/Jun/2012" was handwritten below the signature. However, it was not clear whether the signature was a Mr or a Mrs R.
4. The file "SMS.docx" contained what looked like SMS messages exported from a mobile phone. The contents of the messages were information on "receiver names", deposited amounts, and instructions to withdraw and resend amounts of money. All of the messages were received from a single number. The following are samples of the messages:

From: +97150xxxxxxx
Received: Nov 22, 2012 14:57
Subject: New payment updste.

New payment updste. This is to inform u that 55,120 AED has deposited to ur account , we shall update on what to do. Thank u.

From: +97150xxxxxxx
Received: Nov 22, 2012 14:57
Subject: Please kindly proceed to your bank...

Please kindly proceed to your bank now and withdraw the sum of 50,000 AED, After u have withdraw kindly send 25,000 AED to the same details. MON NASY.

From: +97150xxxxxxx
Received: Nov 22, 2012 14:58
Subject: Receivers Name; ORN BUNTHON,

Receivers Name; ORN BUNTHON, Country ; Cambodia, City; Phnom Penh.

From: +97150xxxxxxx
Received: Nov 22, 2012 14:58
Subject: This is to inform u that 780 AED...

This is to inform u that 780 AED Payment has been deposited to ur account.

From: +97150xxxxxxx
Received: Nov 22, 2012 14:58
Subject: Here is the company balance 5,

Here is the company balance 5,900 AED, plz proceed to ATM and withdraw it now

From: +97150xxxxxxx
Received: Nov 22, 2012 14:58
Subject: Receivers Name; ORN BUNTHON,

Receivers Name; ORN BUNTHON, Country ; Cambodia, City; Phnom Penh.

From: +97150xxxxxxx
Received: Nov 22, 2012 15:00
Subject: This is to inform you that a...

This is to inform you that a payment have been deposited to ur account, Amount; AED 98,949.00, depostor full name; [Ms A].

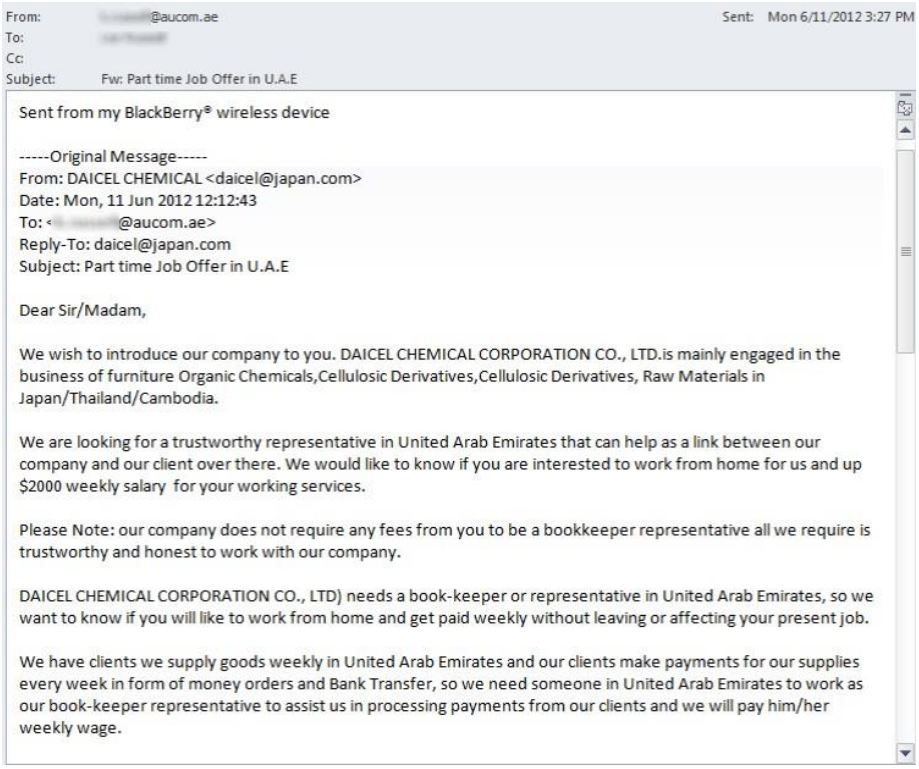
From: +97150xxxxxxx
Received: Nov 22, 2012 15:01
Subject: Out of the payment we want u to...

Out of the payment we want u to proceed and withdraw 92,750 AED out of the payment in ur account.

5. The file "Copies of transfer slips.pdf" contained four scanned documents of money transfer slips performed through Western Union. The transfers were performed on the 15,16,and 18/Jun/2012 as follow:
    a. On 15/Jun/2012 an amount of 1,553.25 US Dollars was transferred by Mrs R to MON NASY in Cambodia. The transfer was done through a branch of Al Ansari Exchange.
    b. On 16/Jun/2012 an amount of 25,000 UAE Dirhams was transferred by Mrs R to ORN BUNTHON in Cambodia. The transfer was done through a branch of

c. On 16/Jun/2012 an amount of 6,503.47 US Dollars was transferred by Mrs R to MON NASY in Cambodia. The transfer was done through a branch of Al Ansari Exchange.
d. On 18/Jun/2012 an amount of 1,526 US Dollars was transferred by Mrs R to ORN BUNTHON in Cambodia. The transfer was done through a branch of Al Ansari Exchange

Eight emails were extracted from the Microsoft Outlook folder residing in the directory C\Users\Sony_vaio\AppData\Local\Microsoft\Outlook\ of the first laptop. A review of the emails showed that four of the emails had the same content (the emails were forwarded from one of Mrs R's email addresses to the other). The earliest email was received on 11/Jun/2012 which included the job offer and description. It also included an application form for the job. The email was originally sent to Mr R's email address, who then forwarded it to Mrs R's email. Figures 7.4 and 7.5 and are copies of the email.



From: [redacted]@aucom.ae Sent: Mon 6/11/2012 3:27 PM
To: [redacted]
Cc:
Subject: Fw: Part time Job Offer in U.A.E

Sent from my BlackBerry® wireless device

-----Original Message-----
From: DAICEL CHEMICAL <daicel@japan.com>
Date: Mon, 11 Jun 2012 12:12:43
To: <[redacted]@aucom.ae>
Reply-To: daicel@japan.com
Subject: Part time Job Offer in U.A.E

Dear Sir/Madam,

We wish to introduce our company to you. DAICEL CHEMICAL CORPORATION CO., LTD.is mainly engaged in the business of furniture Organic Chemicals,Cellulosic Derivatives,Cellulosic Derivatives, Raw Materials in Japan/Thailand/Cambodia.

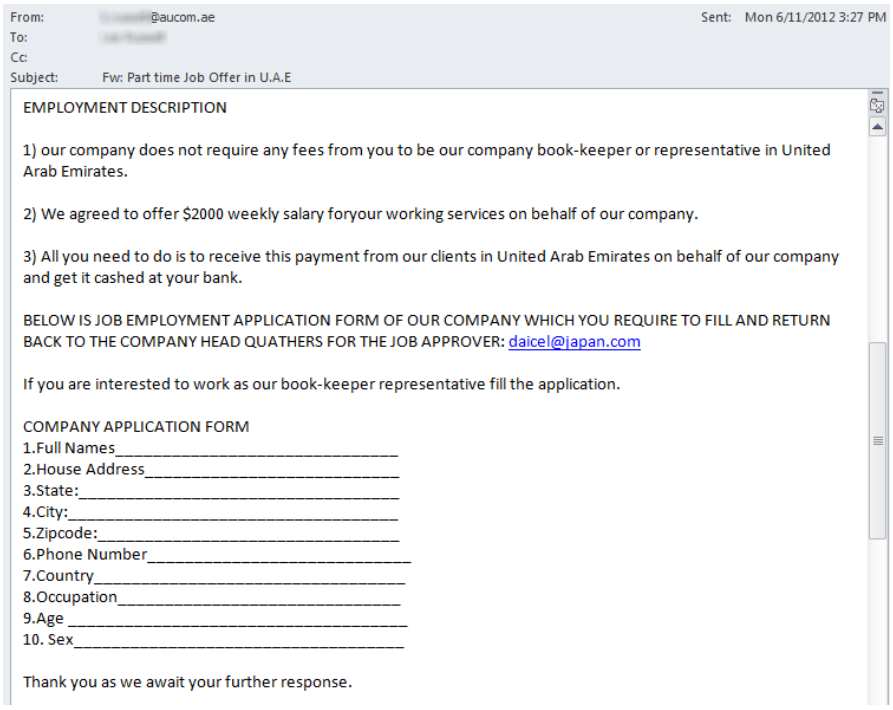
We are looking for a trustworthy representative in United Arab Emirates that can help as a link between our company and our client over there. We would like to know if you are interested to work from home for us and up $2000 weekly salary for your working services.

Please Note: our company does not require any fees from you to be a bookkeeper representative all we require is trustworthy and honest to work with our company.

DAICEL CHEMICAL CORPORATION CO., LTD) needs a book-keeper or representative in United Arab Emirates, so we want to know if you will like to work from home and get paid weekly without leaving or affecting your present job.

We have clients we supply goods weekly in United Arab Emirates and our clients make payments for our supplies every week in form of money orders and Bank Transfer, so we need someone in United Arab Emirates to work as our book-keeper representative to assist us in processing payments from our clients and we will pay him/her weekly wage.

Figure 7.4 The first part of the job offer email.



From: [redacted]@aucom.ae Sent: Mon 6/11/2012 3:27 PM
To: [redacted]
Cc:
Subject: Fw: Part time Job Offer in U.A.E

EMPLOYMENT DESCRIPTION

1) our company does not require any fees from you to be our company book-keeper or representative in United Arab Emirates.

2) We agreed to offer $2000 weekly salary foryour working services on behalf of our company.

3) All you need to do is to receive this payment from our clients in United Arab Emirates on behalf of our company and get it cashed at your bank.

BELOW IS JOB EMPLOYMENT APPLICATION FORM OF OUR COMPANY WHICH YOU REQUIRE TO FILL AND RETURN BACK TO THE COMPANY HEAD QUATHERS FOR THE JOB APPROVER: daicel@japan.com

If you are interested to work as our book-keeper representative fill the application.

COMPANY APPLICATION FORM
1.Full Names_____
2.House Address_____
3.State:_____
4.City:_____
5.Zipcode:_____
6.Phone Number_____
7.Country_____
8.Occupation_____
9.Age _____
10. Sex_____

Thank you as we await your further response.

Figure 7.5 The second part of the job offer email.

The application form (Figure 7.5) was complete with details of Mrs R and sent to the company's email address on the 12/Jun/2012. The email title was "COMPANY APPLICATION FORM". An untitled email was sent from Mr R's email address to Mrs R's email address on the 13/Jun/2012. The email included the HSBC bank account details of Mr R (i.e., his name and account number). Attached to the email was a PDF file that constituted the signed scanned contract agreement of the job. The same email was forwarded from Mrs R's email address to the company's email address, with a sentence that said:

> *Thank you for your offer. Please find attached my signed copy of the employment contact.*

A final email was sent from Mrs R's email address to the company's email address on the 18/Jun/2012. The email read:

> *I would like to advise you that I will be traveling abroad for three weeks leaving on Wednesday 20th June. During this time I will be able to do internet bank transfers only.*
>
> *Additionally please let me know when and how I will be paid for the week I've just completed.*

7.4.2.3.2 Timeline Analysis & Mapping

The timeline was important in this case to establish the chronological order of events. The email correspondence that was extracted from the first laptop (C\Users\Sony_vaio\AppData\Local\Microsoft\Outlook\) was partly consistent with the statements made by Mr R regarding his wife's employment with a foreign company. Organising the emails chronologically showed the following sequence of events:

1. Mr R received the part time job offer letter on the 11/Jun/2012 from the fraudulent company and forwarded it to Mrs R's email address.
2. Mrs R filled in the application form and emailed it back to the company.
3. The company replied to Mrs R with an email stating that she has been granted the job. The email also included the terms and conditions of the job, asked Mrs R to provide a valid bank account number, and provided a contract to be signed by Mrs R.
4. Mr R emailed his bank account details along with a signed contract to Mrs R who forwarded it to the company.
5. The final email (dated 18/Jun/2012) showed that Mrs R had effectively started her job as she had completed a week of assigned work (not specified in the email).

The dates and times of the messages shown in the "SMS.docx" file mentioned in the previous section were also analysed. It was noticed that all of the messages had a "received" date of 22/Nov/2012 with the messages being received minutes apart. This finding will be further elaborated on in the next section.

7.4.2.4 Phase 4: Interpretation and Reporting

In order to conduct a proper interpretation of the offence at hand, all of the related evidence had to be carefully analysed. Also, all possible relationships between the different pieces of evidence had to be identified and established.

Content analysis and timeline analysis of the email correspondence showed that Mrs R had effectively started her part time employment with the fraudulent company on the 13/Jun/2012. She had been given some assignments which she performed during the first week of her job. It was interpreted that Ms A was the first victim whose stolen money went into the account of Mr R to then be laundered by Mrs R.

The statement provided by the victim (Ms A) was consistent with the evidence. The HSBC bank statement (FileDownloadServlet.pdf) showed three transactions that came from Ms A's bank account. The total sum of the transactions was 154,849, which was exactly as Ms A had stated. The contents of the SMS.docx file also corroborated Ms A's statement. Three of the messages

stated the exact amount of money that was stolen from Ms A's account and transferred to Mr R's account:

> *New payment updste. This is to inform u that 55,120 AED has deposited to ur account , we shall update on what to do. Thank u*
>
> *This is to inform u that 780 AED Payment has been deposited to ur account.*
>
> *This is to inform you that a payment have been deposited to ur account, Amount; AED 98,949.00, depostor full name; [Ms A].*

As mentioned in the content analysis and the timeline analysis & mapping sub-phases (Sections 7.4.2.3.1 and 7.4.2.3.2), the SMS messages contained within the SMS.docx file had a "received" date of 22/Nov/2012 with the messages being received minutes apart. Also, all of the messages were received from a single number. A possible interpretation of this issue was that the SMS messages had been forwarded from the original mobile phone to another mobile phone on the 22/Nov/2012 before they have been exported to the laptop. It is worth noting here that if the case was an ongoing investigation, it would be required to ask for the mobile phone that held the original SMS messages. Since the messages were found as text in a document file, they cannot be considered as concrete evidence. However, it is used in this case study for the purpose of explaining how the different pieces of evidence can be linked to reconstruct the crime events.

The contents of the file "Copies of transfer slips.pdf" were also consistent with the withdrawal amounts shown on Mr R's HSBC bank statement file (FileDownloadServlet.pdf), and with the amounts that Mrs R was instructed to withdraw and resent through money exchange service (SMS.docx). It was also consistent with names provided in the SMS messages to whom the money was sent to. It also included confirmation that the money was transferred to the specified receivers. The following are samples of the SMS messages:

> *Receivers; Mon Nasy. Country; Cambodia, City; Phnom Penh.*
>
> *399-633-5634 Mon Nasy 1553.25 USD*
>
> *Please kindly proceed to your bank now and withdraw the sum of 50,000 AED, After u have withdraw kindly send 25,000 AED to the same details. MON NASY.*
>
> *I have sent the funds as requested. Ref: 316-659-0807 Mon Nasy 6503.47 USD. Please advise regarding the remaining 25000 cash*
>
> *Receivers Name; ORN BUNTHON, Country ; Cambodia, City; Phnom Penh.*

Combining all the evidence, there was a strong indication that Mrs R was another victim of the fraud scheme that aimed to use her as a money mule to launder illegally acquired funds from other victims of fraud. The interpretation of all the extracted evidence resulted in:

1. Supporting the first hypothesis that the offence was part of a larger fraud scheme which involved other individuals.
2. Supporting the hypothesis that Mr R was being truthful about the recent employment of his wife (which was with the fraudulent company).
3. Refuting the hypothesis that Mr and Mrs R were part of the scheme.

It was concluded that the unsuspecting Mrs R was used as a money mule. She received and transferred the money illegally acquired from the victim's compromised bank account on behalf of the real offender. She was recruited through a fraudulent online offer of employment, which was sent to Mr R's email address. The real money laundering offender used Mrs R to distance themselves from the source of the stolen money.

An interesting point related to this case was the speed within which Mrs R accepted the job offer. As the emails showed, the employment offer was received on the 11/Jun/2012. Mrs R took the job straight away by filling in the application form and resending it to the company, and providing all the required information (e.g., bank account detail, signed contract). She was effectively in her job by the 13/Jun/2012. Lack of job interview and CV request might make the individual feel suspicious, however, this was not the case with Mrs R. One interpretation of this was that Mrs R was desperate to gain employment. Her vulnerability may have reflected that she was experiencing financial problems. It may also be the case that she was unable to distinguish between legitimate and fraudulent opportunities, and acted on what appeared to be a good opportunity. However, both Mr R and Mrs R failing to identify this fraud potentially raises some suspicion. It is also possible that at some point Mr and Mrs R became aware or suspected that they were part of an illicit scheme, but decided to carry on for the monetary gain.

7.4.3 Discussion

The case studies demonstrated the benefit of the combined approach of standard digital forensics and BA in providing interpretative and investigative utility. This section discusses these benefits by comparing the results in the original case files of the first case study to the outcomes of the examination conducted by the researcher using the proposed model.

For the elaborated case (see Section 7.4.1), the original case file showed that the investigation ceased once evidence related to accessing Miss X's Facebook and performing activities were discovered on Mrs Y's laptop. The report listed the same technical information found by the researchers (see Section 7.4.1.3 for full details) which included the 376 entries in the index.dat

file, the location of the file, and the entries showing that access has been gained to Miss X's Facebook account.

The results section of the original report, however, only listed these findings and no attempts were made to search for the emails of Miss X's office colleagues or roommate. Also, no opinion or hypothesis was provided to explain what might have happened, or to comment on a possible motivation. This might be due to factors such as: (1) following the request letter literally; which only asked to identify whether the seized laptops had been used to login to Miss X's Facebook account and post the defamatory information (2) time constraints, and (3) work overload. The original investigation might have used some aspects of BEA analysis to reach to the final conclusion (e.g., timeline analysis). However, it might have been performed in an ad-hoc manner, and without the investigators being aware of the utility of BEA strategies. The involved DF practitioner might have relied on their expertise and experience in the field to perform the post-mortem examination and analysis of the laptops in question. Notes on the case file showed that the digital forensics examination and analysis of the laptops took 13 working days to conduct. It also showed that examination started on the laptops belonging to the initial main suspect (Mr Y).

The obvious main differences that can be inferred from the DF investigation performed by the main researcher and the original digital investigation performed can be summarised as follows:

1. The original investigation did not prioritise the devices. It started with Mr Y's laptops, and there was no indication of any steps performed to triage and decide which laptop to start with. Performing the prioritisation step could have reduced the time and effort spent on the examination and analysis of the laptops by eliminating full examination of Mr Y's laptop. Following the described procedure took approximately 5 days to finalise the examination and analysis of the laptops in question which was significantly shorter than the 13 days taken in the original investigation.
2. The original investigation did not examine the association between Mrs Y and Miss X's work colleagues. It did not investigate other potential suspects not explicitly named beforehand. As a result, the correspondence between Mrs Y and Miss X's work colleague was not found. On the other hand, the examination and analysis performed in this study went further to investigate the relation of other suspects connected to the offence.

The proposed model is an investigative tool that DF practitioners can utilise for the investigation of interpersonal cases. The model provided here outlines an organised and systematic approach to conducting the post-mortem investigation of the laptops in question. The Review phase enabled the researcher to establish a clear context for the different aspects of the

incident. The incident was categorised in terms of criminal conduct and complexity. The victim's daily routines were assessed to develop theories about factors which created opportunities for victimisation, and possible offender motivations were also considered. This phase also enabled the researcher to formulate a number of hypotheses about identity of probable suspect(s), independent on what was identified on the case request letter. These were later confirmed or refuted based on the evidence identified in later phases. Prioritising the devices also helped to speed up the investigation and reduce associated resource allocation. Starting with Mr Y's laptops would have consumed more time and exhausted the available resources without providing positive results.

Aside from the results that were consistent with those identified in the original investigation report, a key outcome of the analysis was the discovery of the correspondence from Miss X's office colleague. The interpretation of its content was of high investigative value to the case. It provided the researcher with a number of investigative directions: (1) it enabled the researcher to confirm a connection between Mrs Y and Miss X's office colleague, (2) it identified Miss X's office colleague as a probable second-suspect, (3) It provided possible motivation for the offence (jealousy and rage). The original investigation might have identified this information in other ways (e.g., during later interrogation of Mrs Y), however, the discovery and interpretation of the emails made this information available in a shorter time with less effort. Having this concrete evidence could have provided strategies for interrogations and a means to direct the questioning and refute lies.

7.4.4 Limitation

The use of a case study strategy (see Chapter 3 for full descriptions of the study design) enabled the researcher to provide a step-by-step description on *how* to follow the phases and sub-phases of the behavioural DF model. It also enabled the illustration of the usability and benefits of utilising the model in DF investigations. However, due to lack of enough description in the original police documents, the researcher could not assess how following the proposed model in investigating the sample cases differed from the method that was followed in the original investigation of the cases.

The researcher was not able to use comparative analysis with the model testing. In an initial plan, the researcher intended to recruit a group of volunteers from the Electronic Evidence Department at the Dubai Police (approximately 10). The volunteers were to be categorised into three groups: (1) new practitioners with a year or less of experience; (2) practitioners with 2 to 7 years of experience; (3) practitioners with over 7 years of experience. They were to be given a duplicate case of each specified type of interpersonal crime and asked to find relevant evidence, first by using their own procedures, methods, and critical analytic skills; secondly, by following

the proposed model for each case. The tests were to verify: (1) the inferences which can be made about behavioural and motivational characteristics of the crime, offender(s) and victim(s) using the different models; and (2) whether the proposed model developed on the will improve examination time, and the amount and quality of the evidence collected compared to the existing methods used by the practitioners. Three practitioner groups were to be used to: (1) enable an examination of potential differences in the efficacy of the tested model for practitioners with different levels of experience, (2) obtain feedback and comments from practitioners with different levels of experience on the structure and efficacy of the models, and (3) determine their utility for training new practitioners. However, this evaluation could not be performed due to the busy schedule of the DF practitioners and the time constraints of the research. As such, the benefits of conducting this evaluation could not be obtained.

7.5 Summary

This chapter addressed the final objective of the thesis: identify the phases and sub-phases required to perform efficient examination, analysis and interpretation of digital evidence for computer-facilitated interpersonal crimes. A DF investigation model that incorporates aspects of BA was developed. It aimed to provide a practical, structured, multidisciplinary approach into performing DF investigations of computer-facilitated interpersonal crimes. It employed two case studies to illustrate the applicability and utility of the model.

The next chapter provides a general discussion on the work conducted in this thesis.

8 GENERAL DISCUSSION

8.1 Introduction

Behavioural Analysis (BA) has been recognised to aid with the Digital Forensics (DF) investigation process. However, the literature shows limited use of BA in DF investigations. A review of previously developed DF investigation models indicated a lack of sufficient consideration of the behavioural and motivational dimensions of offending, and the way in which digital evidence can be used to address these issues during the investigation process. The research sought to expand on previous work by employing a multidisciplinary approach to extend phases in current DF investigation models by incorporating more consideration to aspects of BA. To fulfil this aim, the researcher identified four main objectives:

1. Examining the usability and applicability of BA in the examination, analysis, and interpretation of digital evidence.
2. Examining the ability of BA to contribute to theoretical understanding of the motivational and behavioural dynamics of computer-facilitated interpersonal crimes.
3. Examining the current use and perceived evidential value of BA in policing and law enforcement.
4. Integrating the findings of the preceding objectives into a usable DF investigation model that incorporates aspects of BA by identifying the phases and sub-phases required to perform the examination, analysis and interpretation of digital evidence for computer-facilitated interpersonal crimes.

The research employed a mixed-methods approach to address each of the thesis objectives. First, it explored the usability and applicability of BA within the post-mortem examination, interpretation, and analysis of digital evidence in computer-facilitated interpersonal crimes.

Specifically, it empirically examined the application of BA in real cases obtained from Dubai Police. It then explored the current use and perceived utility of BA within a sample of national and international population of DF practitioners. The thesis subsequently packaged this obtained knowledge into a usable BA-driven DF investigation model that incorporated aspects of BA to provide a structured guideline into performing the process in a post-mortem investigation of computer-facilitated interpersonal cases. A summary of the conducted work, main results and conclusions are presented in the next sections.

8.2 Summary of the Conducted Work

The review of literature in Chapter 2 showed that behavioural analysis of crime scenes had a long history of being used as a supportive investigative tool in various categories of conventional crimes (e.g., rape, homicide) (Beauregard et al., 2017, Lowe, 2002, Tonkin et al., 2017). A number of studies also recognised it to have similar benefits in investigating computer-facilitated crimes (Bryant, 2016, Rogers, 2003, Turvey, 2011), yet very limited work has been published to show its practical application and benefits in real criminal cases. A review of twelve prominent DF investigation process models that have been proposed between 2001 and 2016 showed a general limitation of disregarding the human element and the lack to consider offender behavioural aspects when investigating computer-facilitated crimes. Another two DF investigation process models were identified to have attempted to implement aspects of BA within the digital forensics investigation of interpersonal crimes, specifically SEIC and cyberstalking crimes: (1) Digital Forensics Profiling Methodology for Cyberstalkers (Silde and Angelopoulou, 2014), and (2) Roger's Behavioural Analysis Model (Rogers, 2015). These two models were reviewed as they offered a useful insight into the development of the proposed behavioural DF investigation model proposed in Chapter 7.

In Chapters 4 and 5, the researcher addressed the two first objectives of the programme of research. Two empirical studies were conducted to explore the application and usability of BA (with a specific focus on the four stages of BEA) during the post-mortem examination, interpretation, and analysis of digital evidence in two categories of computer-facilitated interpersonal crimes: (1) the possession and dissemination of Sexually Exploitative Imagery of Children (SEIC), and (2) cyberstalking. The studies were conducted on a sample of 35 real crime cases obtained from the archives of the Dubai Police. Results showed that not all stages of BEA could be applied to every examined case in the sample, however, the implications of the benefits of BEA when investigating other variations of cases were discussed. A number of benefits were identified with a main outcome presented in two tables providing possible interpretations of potential evidence related to the two crime categories (Tables 4.4, and 5.6). The studies also discussed the four stages of BEA (equivocal evidence analysis, victimology, crime scene characteristics, and offender characteristics) in relation to their applicability and

usefulness in the conducted examination of the sample cases. The two studies also examined the characteristics, behaviours, and motivations of SEIC and cyberstalking offenders, and compared this to the currently available relevant research evidence.

Chapter 6 addressed the third objective of the programme of research. An online questionnaire was administered to empirically measure the perceptions of national and international digital forensics practitioners regarding the use and utility of BA, with a focus on the sub-category of BEA, during the process of investigating SEIC and cyberstalking cases. While approximately half of the participants reported having at least basic knowledge of BEA, and acknowledging its potential contribution to a number of aspects of DF investigations, their daily investigative activities involved a limited use of this technique. Potential interpretations of the findings were conducted leading to the identification of a number of factors that might have limited the utilisation of BA. One identified factor was the lack of proper knowledge on applying BA within the DF investigation process, which emphasised the need to provide guidelines and illustrations on how to utilise BA in DF investigations.

Results from the conducted studies informed the development of BA-driven DF investigation model that integrated aspects of BA (Chapter 7). The model extended the previous work of researchers (i.e., Rogers, 2015, Silde and Angelopoulou, 2014) and provided a practical, structured, multidisciplinary approach into performing a post-mortem examination, analysis, and interpretation of the contents of the digital devices associated with computer-facilitated interpersonal crimes. To illustrate the application and investigative importance of the model, two case studies were conducted on two real cases of computer-facilitated interpersonal crimes.

8.3 Comparative Analysis of Results from the Conducted Studies

Considering aspects of BA within the standard DF investigation process in examining the SEIC cases, the cyberstalking cases, and the two case studies as detailed in the previous chapters of the thesis appeared to be useful in a number of ways. Five investigative benefits of integrating BA into the digital forensics investigation of the cases were identified: (1) focus, speed, and investigative directions, (2) infer victim/offender behaviours, (3) identify offender motivation(s), (4) identify potential victims, and (5) eliminate suspects. Examples of the interpretive and investigative utility of the different types of analysed digital evidence are provided in this section to demonstrate the value of this combined approach.

8.3.1 Focus, Speed, and Investigative Directions

In one cyberstalking case, the victim reported (in the background documentation of the case) suspicious activity on her computer stating that messages containing hateful words were

popping up on her screen. The victim suspected two people with whom she used to have online relationships. A quick review of the installed software on her computer showed that it did not have any anti-virus software, which indicated limited understanding of how to protect her computer. To start with, a virus scan was run to scan for malicious software. The result showed a list of malicious files and their logical locations on the computer. One of the files was a Trojan horse virus; a disguised malicious software that enables hackers to gain remote access to the compromised computer. This indicated that her machine was indeed compromised and could be remotely accessed. A review of the malicious files and their locations showed that the Trojan horse file was located in the download folder of a specific chat client software that the victim used. Examining the chat logs indicated that one of the people whom she suspected had sent her this file. This indicated that the victim naively downloaded and ran the malicious file without checking it first, which put her at risk of victimisation.

This example demonstrates how BA can benefit an investigation by providing a specific focus and direction for subsequent search strategies, as well as understanding the behavioural characteristics of the victim and offender. These benefits had been identified in the literature by a number of researchers (e.g., Bryant, 2016, Casey et al., 2014, Turvey, 2011) It is very important to understand the context of the offence before starting to analyse the digital device to identify relevant evidence. This can assist the digital forensics practitioner in identifying the starting point for evidence recovery rather than an ad hoc, unfocused search of a huge number of potentially relevant files (Rogers, 2015, Turvey, 2011). This also demonstrates that BA has utility in triage techniques and directing the investigator to locations of potential evidence (Silde and Angelopoulou, 2014).

8.3.2 Infer Behaviours of Victim/Offender

In another case, the offender created a fake profile in the victim's name on a dating website. He uploaded indecent pictures of the victim, and posted fabricated explicit messages detailing her sexual fantasies and soliciting visitors to contact her to engage in sexual acts. He also posted her email address. The victim reported a suspect to the police.

Examining the victim's online activities (through web browser cache and history files) indicated that she was a regular visitor to the dating website in question. In the interview transcript, the victim stated that she had met the suspect online through this site, and had a brief relationship with him which she ended. Examining the chat logs of her most recent conversations with the suspect showed a steady flow of messages from the suspect that started with words of love, trying to re-establish relationship with her, which then gradually shifted to words of anger and intense emotional responses.

Honey why don't you answer my emails, hope you are fine.

Honey I changed my email because so many ladies are disturbing me I don't want to lose you.

Why aren't you replying?!! Are you with someone else?!

Bad girl you are not answering me or are you busy [f@#king] a man on webcam.

You damned W@#RE!!! You will regret you ever ignored me!!

Examining the suspect's computer indicated that it had been used to log into the victim's fake profile several times. The suspect's computer also had copies of pictures of the victim that had been uploaded to the profile, apparently to seek revenge for their failed relationship.

The previous example demonstrates how digital evidence can reflect the behaviours of the victim/offender, which help understanding the dynamics of the crime. In this case, the victim's regular visits to the dating website and meeting people she had met online in the offline environment increased her risk of victimisation.

Written online communications can reveal useful evidence in computer-facilitated interpersonal crimes. In terms of behaviour, it indicates signature behaviours of the offender (e.g., repeated syntax, spelling, grammar mistakes, nicknames) (Casey et al., 2014, Rogers, 2015, Turvey, 2011). In terms of investigative utility, it provided evidence of the victim/offender relationship, which helps understand the context of the crime and identify the most probable offender (in cases having more than one suspect).

As for the SEIC sample cases, written communications were not available as the suspects did not conduct any online communications related to the offence. However, in cases where this information is available it can help identify signature characteristics of the offender (e.g., repeated syntax, spelling, grammar mistakes, nicknames). This can help identify the offender in cases of having multiple users of the computer. It can also reveal the motivation/intentions of the offender as they express it to their like-minded online friends (e.g., victim preferences). It can also identify links and traces to other possible suspects. Finally, it can reveal online communication with offender networks or potential victims.

User files and folders, as well as web browser cache and history files, are also useful in SEIC and cyberstalking cases. They can indicate the victim's interests and lifestyle (e.g., search terms, regularly visited social networks) which might have exposed them to the offender and victimisation. They can indicate offender's interests and related offence motivations. These files can also identify links/traces to other possible victims/suspects, as well as other evidence

indicating that an offence occurred. For example, in one cyberstalking case the offender's computer had a user-created folder that stored files of morphed explicit images of the victim, plus the original picture of the victim, and evidence of using specific software to create those images.

In one SEIC case, the suspect claimed accidental access to the SEIC materials while surfing the internet. His claim might have been accepted if the SEIC files were few. An examination of the web browser cache and history files, however, revealed evidence that challenged his claims. Over 400 files of SEIC were found in the cache folder. Plus, the history files showed that the suspect had visited SEIC related websites many times and on different dates. Since there were no SEIC files in other locations on the suspect's computer, the evidence indicated that the suspect intentionally viewed SEIC, without the purposeful act of downloading or saving them to his device.

8.3.3 Infer Motivation of Offender

Digital evidence can also indicate the motivation(s) of the offender (e.g., revenge, money gain). For example, the offender's written communications illustrated in the preceding section, and the creation of the obscene fake profile for the victim indicated that the most obvious motivation was to seek revenge for a failed relationship. Analysing written communication can also provide an insight into the motivation of the offender. Table 5.5 provides some illustrative quotations extracted from the written communication from the sample cases, and reflect the motivations of the offenders.

Depending on the specific type of the offence, the number of files, where they are stored, as well as the presence of files containing paraphilic materials, can also indicate the offender's existing deviant sexual interests. This can add to the profile of the offender by providing further evidence of the motivation for their behaviour. For instance, the presence of SEIC files on the hard-disk of a suspect accused of cyberstalking an underage victim may suggest that they had a sexual motivation for their behaviour. This had been identified in the literature as using SEIC to nurture the offender's existing or developing sexual interests in children, and the use of the collected imagery as part of a contact offending (Beech et al., 2008).

8.3.4 Identify Potential Victims

Sorting and categorising victims' files indicates offender commitment to their behaviour as represented by the time and effort taken to organise victim information. It also provides evidence about other current or potential victims. In one of the cyberstalking cases, evidence showed that the current victim was not the only person targeted by the offender. An examination of the offender's computer indicated that they had created a folder with subfolders

that included different information and pictures of three females in addition to the victim that reported him.

Depending on the type of cyberstalking and other factors (e.g., file types and location, timestamps, deleted files on the offender's computer), digital evidence can provide indications of other offence-related behaviour. For example, if the deleted files were pictures of the victim or victim-related data that were originally stored in a user created directory, this would indicate the offender's specific interest in the victim. It can also indicate their intention to cyberstalk the victim, and then deleting the crime-related files to evade detection.

As with SEIC cases, behavioural analysis did not show a direct link to identifying potential victims. However, behavioural analysis of specific types of digital evidence has the potential to help identify the selection of victims. For example, written communications can indicate on offender's criteria for selecting their victim (e.g., being easily controlled, close physical location to the offender). Examining the techniques used by the offender to solicit their victims (e.g., use of fake personas, expressing affection) can lead to the development of online monitoring strategies to prevent further victimisations.

8.3.5 Eliminate Suspects

In a final case, the offender harassed the victim by impersonating her on a Facebook account and posting her pictures accompanied with offensive comments. Her main suspect was her ex-husband who had remarried after their divorce. Examining the ex-husband's computer showed a folder that contained her pictures posing either alone, or alongside with the ex-husband and their daughter. Analysing the web browser history proved that the Facebook account in question has been logged into many times. At this point, the evidence seemed to support the victim's suspicion that her ex-husband was to blame. However, performing a timeline analysis identified periods of intense activity on the Facebook account, which were mostly during week days between 9:00am and 2:00pm. Since the ex-husband worked during this period of the day, the only other possible offender with access to the same computer was the new wife, who was at home during this time window.

In order to maximise the investigative value of the collected digital evidence, a timeline analysis must be conducted (Rogers, 2015). Evidence files must not be examined separately. Whenever possible, associated dates and times of the collected data must be correlated to other time stamps (e.g., from statements of the victim and offender). This can provide a timeline for the activities involving the offender and victim that can aid in the reconstruction of the crime. It can also provide a timeframe of activities that can be checked against the claims of the victim/offender. Variation in a file's time stamp can indicate user treatment of the file (e.g.,

whether they had altered an innocent picture of a victim into an obscene image). Time stamps can also suggest how long the offender has been in possession of specific files and the length of time they were planning cyberstalking the victim(s). Finally, correlating file time stamps with the daily activities of suspects can help determine the probable offender in cases where multiple suspects use the same computer (Rogers, 2015).

8.4 Methodological Approach

The research used a mixed-methods approach which was particularly relevant for the current research programme as it aimed to address different types of research questions. It complemented the research process as the different qualitative and quantitative methods built on each other's strengths and limitations (Creswell and Creswell, 2017). For example, the two parts of Study 1 presented in Chapters 4 and 5 employed a mixed-methods approach with quantitative and qualitative analysis of relevant digital evidence and case documentation. This design was most appropriate for these studies given the time constraints and limited amount of resources (i.e., cases). This was also useful in developing empirical evidence on the usability and utility of BA on the investigated cases.

In Chapter 6 (Study 2), using the online questionnaire was an effective means of recruiting a larger and a diverse sample of national and international DF practitioners. The questionnaire collected quantitative and qualitative data. The quantitative data was used to measure a number of variables such as the perceived utility and the daily use of activities that constitute BA during the DF investigation of specific crimes. The qualitative data aided in gaining a better understanding of the investigators perceptions of the utility of BA, and in identifying factors that limits its use.

In Chapter 7 (Study 3), two case studies were used to provide a descriptive, in-depth analysis of each case, and provide a clear step by step guide on how to apply the different phases and sub phases of the model.

In order to assess the reliability and validity of the outcome of each of the conducted studies and to minimise bias, the researcher sought to address four criteria: (1) credibility, (2) transferability, (3) dependability, and (4) confirmability (Lincoln and Guba, 1985) (see Chapter 3, Section 3.5.3). The issues of credibility, transferability and dependability were addressed by providing a detailed description of the study's design, and the procedures followed for data collection and analysis. The use of a mixed-methods approach was utilised to select appropriate procedures that address the different questions of the studies. The use of *real* crime cases in testing the applicability and utility of the integrated procedure of DF and BA (in Studies 1 and 3) increases the credibility of the collected data and the findings, as opposed to the use of

fictional scenarios performed in earlier studies identified in the literature (e.g., Silde and Angelopoulou, 2014). Also, in Study 1, the collection and analysis of both qualitative and quantitative data from different case-related sources (i.e., bit-wise image files, case documents, interview scripts of offender(s)/victim(s)) was to achieve triangulation. Furthermore, performing the study in two parts; using a sample of a different computer-facilitated interpersonal crime category for each part, addresses transferability of the results.

Confirmability was addressed by the researcher working with a multidisciplinary supervisory team to discuss the different stages of the studies design, data collection, and data analysis. For Studies 1 and 3, investigating each individual case *afresh*, without reviewing the results in the original case documents also ensured that the findings of the study were not influenced and biased by the results in the original report. The 15 years' experience of the researcher in investigating digital crimes also aided in controlling bias by trying to stay objective through the different stages of investigating the sample cases. Interpretations of the collected evidence (see Chapters 4 and 5, Tables 4.4 and 5.6) were further revised by the researcher and the supervisory team to reach the final output. Finally, both parts of Study 1, and a section of Study 2 were peer-reviewed and published in scientific journals (Al Mutawa et al., 2015, 2016, Franqueira et al., 2018), while Study 3 is under review for publication.

Reliability and validity of the conducted studies were also addressed by recognising the limitations of each study (see Chapter 3).

8.5 Contribution

The contribution of the work performed in this thesis can be summarised by the following:

1. The research advances the state-of-literature by further examining SEIC offenders and cyberstalkers' behaviours, motivations, and *modus operandi*.
2. The research empirically examined the utility and applicability of BA in the DF investigation of 35 *real* computer-facilitated interpersonal crime cases (SEIC and cyberstalking). This increased the understanding of the benefits of BA for the DF investigations and interpretation of digital evidence. Tables of potential interpretations of the digital evidence found within each crime category, and their investigative utility were provided to aid DF practitioners in understanding the potential investigative benefits of the different types of digital evidence.
3. The proposed Behavioural Digital Forensics Investigation Model advances the state-of-practice by incorporating BA in the examination and analysis of digital evidence using real-life cases.

4. The research weaves together offender behaviour and motivation theories into practical application; it bridges the gap between theory and practice.

8.6 Limitations and Future Direction

With regards to the SEIC and the cyberstalking studies detailed in Chapters 4 and 5, the sample cases constituted crimes conducted between 2009-2013. The identified locations of potential evidence, victim/offender behaviours, and offender motivations were based on evidence found in these cases. Examining the usability and utility of BA was also limited by the available digital evidence within the sample cases. As such, the studies were unable to address the most recent tools, techniques, and offending behaviours which might have emerged while the research was underway. Also, it couldn't examine the utility of BA in other forms of these cases (e.g., SEIC cases where the offender is a producer or a groomer). This highlights the need for further studies to examine utility of BA in different variations of recent SEIC and cyberstalking cases.

While the proposed behavioural digital forensics investigation model demonstrated utility in investigating the cases on which it was tested, it wasn't possible to clearly identify how it differed from the original investigation conducted on the cases. Further work is necessary to extend the testing of the proposed model with a larger sample of cases involving different categories of computer-facilitated interpersonal crimes.

Future work should also examine whether it is possible to impose minimum educational and training requirements for DF investigators in relation to making them qualified to employing BA within the DF investigation process. It also worth exploring whether the model can be implemented within the larger DF investigation framework.

8.7 Summary

The programme of research used existing standard practice in the field of digital forensics and integrated different aspects of BA; including the four stages of BEA as defined by Turvey (2011), within the technical examination of the digital evidence. Results showed that using this approach when investigating computer-facilitated interpersonal crimes assisted the investigator in a number of ways. It had the benefit of focusing the investigation, and providing logical directions for identifying the location of further relevant evidence. This increased the efficacy and speed of the investigation. It also enabled a better understanding and interpretation of victim/offender behaviours (e.g., probable offender motivations, amount of planning, victim risk factors), which facilitated an in-depth understanding of the dynamics of the specific crime. Further, in some cases it enabled the identification of potential victims other than the person

originally reporting the crime. Finally, it eliminated suspects in cases where the computer in question was accessed by more than one user through the same user account.

One implication of this work is the ability to show practically that BA can be applied and be of use within the DF investigative process for specific categories of computer-facilitated interpersonal crimes. It has been theorised in the past that BA, including the four stages of BEA can provide investigative value to the DF investigation process (Casey et al., 2014, Rogers, 2015, Turvey, 2011), however, this has not been tested empirically in previous work. It is hoped that the knowledge gathered in this thesis will benefit DF investigators and will provide insight on how BA can be utilised within the DF investigation process. The proposed model should provide sufficient guidelines for DF investigators on how to practically apply each step within the DF investigation process.

REFERENCES

Database of Electronic Crimes. Dubai - United Arab Emirates: Dubai Police; 2014.

Abbasi A, Zhang Z, Zimbra D, Chen H, Nunamaker Jr JF. Detecting fake websites: the contribution of statistical learning theory. Mis Quarterly 2010:435-61.

Ademu I, Imafidon C, Preston D. A new approach of digital forensic model for digital forensic investigation. International Journal of Advanced Computer Science and Applications 2011;2(12):pp. 175-8.

Agarwal A, Gupta M, Gupta S, Gupta SC. Systematic digital forensic investigation model. International Journal of Computer Science and Security (IJCSS) 2011;5(1):118-31.

Aggarwal S, Henry P, Kermes L, Mulholland J. Evidence handling in proactive cyberstalking investigations: the PAPA approach. Systematic Approaches to Digital Forensic Engineering, 2005 First International Workshop on: IEEE; 2005. p. 165-76.

Aghekyan-Simonian M, Forsythe S, Kwon WS, Chattaraman V. The role of product brand image and online store image on perceived risks and online purchase intentions for apparel. Journal of Retailing and Consumer Services 2012;19(3):325-31.

Agustina JR. Understanding cyber victimization: Digital architectures and the disinhibition effect. International Journal of Cyber Criminology 2015;9(1):35.

Ahmad R, Yunos Z, Sahib S. Understanding cyber terrorism: The grounded theory method applied. Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on: IEEE; 2012. p. 323-8.

Ainsworth P. Offender Profiling Crime Analysis: Willan, 2013.

Akdeniz Y. Internet child pornography and the law: national and international responses: Routledge, 2016.

Al Mutawa N, Al Awadhi I, Baggili I, Marrington A. Forensic artifacts of Facebook's instant messaging service. Internet Technology and Secured Transactions (ICITST), 2011 International Conference for: IEEE; 2011. p. 771-6.

Al Mutawa N, Bryce J, Franqueira VNL, Marrington A. Behavioural evidence analysis applied to digital forensics: An empirical analysis of child pornography cases using P2P networks. Availability, Reliability and Security (ARES), 2015 10th International Conference on: IEEE; 2015. p. 293-302.

Al Mutawa N, Bryce J, Franqueira VNL, Marrington A. Forensic investigation of cyberstalking cases using Behavioural Evidence Analysis. Digital investigation 2016;16:S96-S103.

Al Sharif S, Al Ali M, Salem N, Iqbal F, El Barachi M, Alfandi O. An Approach for the Validation of File Recovery Functions in Digital Forensics' Software Tools. New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on: IEEE; 2014. p. 1-6.

Al-Khateeb HM, Epiphaniou G, Alhaboby ZA, Barnes J, Short E. Cyberstalking: Investigating formal intervention and the role of Corporate Social Responsibility. Telematics and Informatics 2017;34(4):339-49.

Alanazi F, Jones A. A Method to Enhance the Accuracy of Digital Forensic in the Absence of Sufficient Evidence in Saudi Arabia. World Academy of Science, Engineering and Technology, International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering 2017;11(3):516-20.

Alexy EM, Burgess AW, Baker T. Internet offenders traders, travelers, and combination trader-travelers. Journal of Interpersonal Violence 2005;20(7):804-12.

Alison L. Forensic Psychologists Casebook: Psychological Profiling and Criminal Investigation: Routledge, 2013.

Alison L, Bennell C, Mokros A, Ormerod D. The personality paradox in offender profiling: A theoretical review of the processes involved in deriving background characteristics from crime scene actions. Psychology, Public Policy, and Law 2002;8(1):115.

Aliyu AA, Bello MU, Kasim R, Martin D. Positivist and Non-Positivist Paradigm in Social Science Research: Conflicting Paradigms or Perfect Partners? Journal of Management and Sustainability 2014;4(3):79.

Altiero RA. Digital Forensics Tool Interface Visualization. Nova Southeastern University; 2015.

Annon JS. Investigative profiling: A behavioral analysis of the crime scene. American Journal of Forensic Psychology 1995.

Antoniou AK, Akrivos D. Prosecutions, Convictions and Sentencing. The Rise of Extreme Porn: Springer; 2017. p. 201-27.

Asghar J. Critical paradigm: a preamble for novice researchers. Life Science Journal 2013;10(4):3121-7.

Ashcroft J. Stalking and domestic violence: Report to Congress. Washington, DC: US Department of Justice, Office of Justice Programs; 2001.

Atefi K, Yahya S, Atefi A. A survey on digital forensics investigation of Seafile as a cloud storage. International Journal of Engineering Research And Management (IJERM) 2014;1.

Atieno OP. An analysis of the strengths and limitation of qualitative and quantitative research paradigms. Problems of Education in the 21st Century 2009;13(1):13-38.

Avison D, Baskerville R, Myers M. Controlling action research projects. Information technology & people 2001;14(1):28-45.

Babchishin KM, Hanson RK, VanZuylen H. Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. Archives of sexual behavior 2015;44(1):45-66.

Balfe M, Gallagher B, Masson H, Balfe S, Brugha R, Hackett S. Internet child sex offenders' concerns about online security and their use of identity protection technologies: a review. Child Abuse Review 2015;24(6):427-39.

Baryamureeba V, Tushabe F. The enhanced digital investigation process model. Digital Forensics Research Workshop. Baltimore, Maryland2004.

Baskerville RL. Investigating information systems with action research. Communications of the AIS 1999;2(3es):4.

Baskerville RL, Wood-Harper AT. A critical perspective on action research as a method for information systems research. Enacting Research Methods in Information Systems: Volume 2: Springer; 2016. p. 169-90.

Beauregard E, Beauregard E, Busina I, Busina I, Healey J, Healey J. Confessions of sex offenders: extracting offender and victim profiles for investigative interviewing. Journal of Criminal Psychology 2017;7(1):13-28.

Beebe NL, Clark JG. A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation 2005;2(2):147-67.

Beech AR, Elliott IA, Birgden A, Findlater D. The internet and child sexual offending: A criminological review. Aggression and violent behavior 2008;13(3):216-28.

Bennett WW, Hess KM. Investigating violent crimes. Criminal investigation

: Cengage Learning; 2007. p. 296-313.

Bocij P. Cyberstalking: Harassment in the Internet age and how to protect your family: Greenwood Publishing Group, 2004.

Bocij P, McFarlane L. Online harassment: Towards a definition of cyberstalking. Prison Service Journal 2002;139:31-8.

Boon J, Sheridan L. Stalking and Psychosexual Obsession–Psychological Perspectives for Prevention, Policing and Treatment: Chichester, 2002.

Boyd C, Forster P. Time and date issues in forensic computing—a case study. Digital Investigation 2004;1(1):18-23.

Braun V, Clarke V. Using thematic analysis in psychology. Qualitative research in psychology 2006;3(2):77-101.

Brown CS. Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology 2015;9(1):55.

Bryant R. Policing digital crime: Routledge, 2016.

Bryce J. ICTs and child sexual offending. The Routledge Handbook of Technology, Crime and Justice 2017:96.

Bryce J, Franqueira VN, Marrington A. Special issue on cyberharassment investigation: Advances and trends. Journal of Digital Forensics, Security and Law (JDFSL) 2016.

Bryce J, Fraser J. The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions. Computers in Human Behavior 2014;30:299-306.

Bryman A. Integrating quantitative and qualitative research: how is it done? Qualitative research 2006;6(1):97-113.

Bryman A. Social research methods: Oxford university press, 2015.

Buchanan T, Whitty MT. The online dating romance scam: causes and consequences of victimhood. Psychology, Crime & Law 2014;20(3):261-83.

Burgess AW, Baker T. Cyberstalking. Stalking and psychosexual obsession: Psychological perspectives for prevention, policing and treatment 2002:201-19.

Burke A, Sowerbutts S, Blundell B, Sherry M. Child pornography and the Internet: Policing and treatment issues. Psychiatry, Psychology and Law 2002;9(1):79-84.

Cafe R. Police detection of child porn images increases by 48%. BBC News2013.

Cahyani NDW, Martini B, Choo KKR, Al-Azhar A. Forensic data acquisition from cloud-of-things devices: windows Smartphones as a case study. Concurrency and Computation: Practice and Experience 2016.

Campbell DT, Stanley JC. Experimental and quasi-experimental designs for research: Ravenio Books, 2015.

Canter D, Youngs D. Investigative psychology: Offender profiling and the analysis of criminal action: John Wiley & Sons, 2009.

Canter DV. Offender profiling. The Cambridge Handbook of Forensic Psychology. Cambridge, UK: Cambridge University Press; 2010. p. 236-41.

Canter DV, Alison LJ, Alison E, Wentink N. The organized/disorganized typology of serial murder: Myth or model? Psychology, Public Policy, and Law 2004;10(3):293.

Carlton GH. A grounded theory approach to identifying and measuring forensic data acquisition tasks. Journal of Digital Forensics, Security and Law 2007;2(1):2.

Carlton GH, Worthley R. An evaluation of agreement and conflict among computer forensics experts. System Sciences, 2009 HICSS'09 42nd Hawaii International Conference on: IEEE; 2009. p. 1-10.

Carnes P. In the shadows of the net: Breaking free of compulsive online sexual behavior: Hazelden Publishing, 2013.

Carrier B, Spafford EH. Getting physical with the digital investigation process. International journal of digital evidence 2003;2(2):1-20.

Carson D. The abduction of Sherlock Holmes. International Journal of Police Science & Management 2009;11(2):193-202.

Casale S, Fioravanti G. Satisfying needs through Social Networking Sites: A pathway towards problematic Internet use for socially anxious people? Addictive Behaviors Reports 2015;1:34-9.

Casey E. Handbook of computer crime investigation: forensic tools and technology. 1 ed: Academic press, 2002.

Casey E. Investigative reconstruction with digital evidence. In: Casey E, Turvey BE, editors. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet: Academic Press; 2011. p. 255-73.

Casey E, Blitz A, Steuart C. Digital evidence and computer crime. Academic Press; 2014.

Cavezza C, McEwan TE. Cyberstalking versus off-line stalking in a forensic sample. Psychology, Crime & Law 2014;20(10):955-70.

Chaski CE. Who's at the keyboard? Authorship attribution in digital evidence investigations. International journal of digital evidence 2005;4(1):1-13.

Chen H, Beaudoin CE, Hong T. Protecting oneself online: The effects of negative privacy experiences on privacy protective behaviors. Journalism & Mass Communication Quarterly 2016;93(2):409-29.

Chen H, Beaudoin CE, Hong T. Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. Computers in Human Behavior 2017;70:291-302.

Chen W, Hirschheim R. A paradigmatic and methodological examination of information systems research from 1991 to 2001. Information systems journal 2004;14(3):197-235.

Chong C-H, Yeo K-J. An Overview of Grounded Theory Design in Educational Research. Asian Social Science 2015;11(12):258.

Choudrie J, Dwivedi YK. Investigating the research approaches for examining technology adoption issues. Journal of Research Practice 2005;1(1):1.

Choy LT. The strengths and weaknesses of research methodology: Comparison and complimentary between qualitative and quantitative approaches. IOSR Journal of Humanities and Social Science 2014;19(4):99-104.

Christensen LB, Johnson B, Turner LA. Research methods, design, and analysis. 2011.

Cifas. Fraudscape 2017: External and internal fraud threats. UK: Cifas; 2017. p. 17.

Clough J. Principles of cybercrime: Cambridge University Press, 2010.

Cohen F. Toward a science of digital forensic evidence examination. Advances in Digital Forensics VI 2010:17-35.

Cohen FB. Digital forensic evidence examination. 5th ed: Fred Cohen & Associates, 2013.

Copson G. Coals to Newcastle? Part 1: A study of offender profiling. London: Home Office, 1995.

Copson G, Badcock R, Boon J, Britton P. Editorial: Articulating a systematic approach to clinical crime profiling. Criminal Behaviour and Mental Health 1997;7(1):13-7.

Cornford T, Smithson S. Project research in information systems: a student's guide: Palgrave, 2006.

Creswell JW, Creswell JD. Research design: Qualitative, quantitative, and mixed methods approaches: Sage publications, 2017.

Danquah P, Longe O. Cyber deception and theft: An ethnographic study on cyber criminality from a ghanaian perspective. Journal of Information Technology Impact [em linha] 2011;11(3):169-82.

Daryabar F, Tadayon MH, Parsi A, Sadjadi H. Automated analysis method for forensic investigation of cloud applications on Android. Telecommunications (IST), 2016 8th International Symposium on: IEEE; 2016. p. 145-50.

Denzin NK, Lincoln YS. Handbook of Qualitative Research. 2000.

Douglas J, Burgess AW, Burgess AG, Ressler RK. Crime classification manual: A standard system for investigating and classifying violent crime: John Wiley & Sons, 2013.

Douglas JE, Ressler RK, Burgess AW, Hartman CR. Criminal profiling from crime scene analysis. Behavioral Sciences & the Law 1986;4(4):401-21.

Draugalis JR, Coons SJ, Plaza CM. Best practices for survey research reports: a synopsis for authors and reviewers. American journal of pharmaceutical education 2008;72(1):11.

Dreßing H, Bailer J, Anders A, Wagner H, Gallas C. Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. Cyberpsychology, Behavior, and Social Networking 2014;17(2):61-7.

Du X, Le-Khac N-A, Scanlon M. Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. arXiv preprint arXiv:170801730 2017.

Dutta D, Tazivazvino C, Das S, Tripathy B. Social Internet of Things (SIoT): transforming smart object to social object. NCMAC 2015 Conference Proceedings2015.

Eckert S. Fighting for recognition: Online abuse of women bloggers in Germany, Switzerland, the United Kingdom, and the United States. New Media & Society 2017:1461444816688457.

Elliott IA, Beech AR. Understanding online child pornography use: Applying sexual offense theory to internet offenders. Aggression and Violent Behavior 2009;14(3):180-93.

Eterovic-Soric B, Choo K-KR, Ashman H, Mubarak S. Stalking the stalkers-detecting and deterring stalking behaviours using technology: a review. Computers & Security 2017.

Etikan I, Musa SA, Alkassim RS. Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and Applied Statistics 2016;5(1):1-4.

European Union Agency for Fundamental Rights. Violence against women: an EU-wide survey. Luxembourg2014.

Fahsing IA, Ask K. In Search of Indicators of Detective Aptitude: Police Recruits' Logical Reasoning and Ability to Generate Investigative Hypotheses. Journal of Police and Criminal Psychology 2018;33(1):21-34.

Ferguson C. Investigative relevance. In: Petherick W, editor. Profiling and Serial Crime: Theoretical and Practical Issues

. 3 ed: Anderson publishing; 2014.

Fetterman DM. Ethnography: Step-by-step: Sage, 2010.

Fisher RP, Geiselman RE, Amador M. Field test of the Cognitive Interview: enhancing the recollection of actual victims and witnesses of crime. Journal of Applied Psychology 1989;74(5):722.

Fisher RP, Geiselman RE, Raymond DS. Critical analysis of police interview techniques. Journal of Police Science and Administration 1987;15(3):177-85.

Flick U. Introducing research methodology: A beginner's guide to doing a research project: Sage, 2015.

Franke K, Årnes A, Flaglien A, Sunde IM, Dilijonaite A, Hamm J, et al. Challenges in Digital Forensics. In: Årnes A, editor. Digital Forensics. Chichester, UK: John Wiley & Sons, Ltd; 2017. p. 313-7.

Franqueira VN, Bryce J, Al Mutawa N, Marrington A. Investigation of Indecent Images of Children cases: Challenges and suggestions collected from the trenches. Digital Investigation 2018;24:95-105.

Fusco CA. Stalking 2.0: The era of cyberstalking. Utica College; 2014.

Gable GG. Integrating case study and survey research methods: an example in information systems. European journal of information systems 1994;3(2):112-26.

Galbreath N, Berlin F, Sawyer D. Paraphilias and the Internet. Sex and the Internet: A guidebook for clinicians 2002:187-205.

Geberth VJ, Bagerth VJ. Practical homicide investigation: Tactics, procedures, and forensic techniques: CRC Press Boca Raton, FL, 1996.

Geiselman RE, Fisher RP. Interviewing witnesses and victims. Investigative Interviewing: Handbook of Best Practices Toronto: Toronto, ON: Thomson Reuters Publishers 2014.

Glaser BG, Strauss AL. The discovery of grounded theory: Strategies for qualitative research: Transaction Publishers, 2009.

Goldkuhl G. Pragmatism vs interpretivism in qualitative information systems research. European journal of information systems 2012;21(2):135-46.

Goulding C. Grounded Theory: some reflections on paradigm, procedures and misconceptions. 1999.

Graves J, Acquisti A, Anderson R. Experimental measurement of attitudes regarding cybercrime. 13th Annual Workshop on the Economics of Information Security Pennsylvania State University2014.

Gregory P, Barroca L, Sharp H, Deshpande A, Taylor K. The challenges that challenge: Engaging with agile practitioners' concerns. Information and Software Technology 2016;77:92-104.

Grispos G, Glisson WB, Pardue JH, Dickson M. Identifying User Behavior from Residual Data in Cloud-based Synchronized Apps. arXiv preprint arXiv:14112132 2014.

Grispos G, Storer T, Glisson WB. Calm before the storm: the challenges of cloud. Emerging digital forensics applications for crime detection, prevention, and security 2013;4(1):28-48.

Guarino A. Digital Forensics as a Big Data Challenge. Isse2013. p. 197-203.

Hammersley M, Atkinson P. Ethnography: Principles in practice: Routledge, 2007.

Hancock DR, Algozzine B. Doing case study research: A practical guide for beginning researchers: Teachers College Press, 2015.

Hancock JT, Woodworth MT, Porter S. Hungry like the wolf: A word-pattern analysis of the language of psychopaths. Legal and criminological psychology 2013;18(1):102-14.

Hango DW. Cyberbullying and cyberstalking among Internet users aged 15 to 29 in Canada: Statistics Canada, 2016.

Harvey D. Cyberstalking and internet harassment: What the law can do. Çevrim-içi: http://www netsafe org nz/Doc_Library/netsafepapers_davidharvey_cyberstalking pdf], Erişim tarihi 2003;29:2011.

Hazelwood RR, Ressler RK, Depue RL, Douglas JC. Criminal investigative analysis: An overview. Practical aspects of rape investigation: A multidisciplinary approach 1995:115-26.

Heinrich PA. Generation iStalk: an Examination of the prior relationship between victims of stalking and offenders. Criminal Justice: Marshall University; 2015. p. 111.

Henry N, Powell A. Technology-facilitated sexual violence: A literature review of empirical research. Trauma, Violence, & Abuse 2016:1524838016650189.

Henry O, Mandeville-Norden R, Hayes E, Egan V. Do internet-based sexual offenders reduce to normal, inadequate and deviant groups? Journal of Sexual Aggression 2010;16(1):33-46.

Henshaw M, Ogloff JR, Clough JA. Looking Beyond the Screen A Critical Review of the Literature on the Online Child Pornography Offender. Sexual abuse: a journal of research and treatment 2015:1079063215603690.

Hewitt C, Marcum CD. Child Pornography. The Encyclopedia of Crime and Punishment 2016.

Higgs T, Carter AJ, Tully RJ, Browne KD. Sexual murder typologies: A systematic review. Aggression and Violent Behavior 2017.

Holder EH, Robinson LO, Rose K. Electronic crime scene investigation: an on-the-scene reference for first responders. Washington2001.

Holmes RM, Holmes ST. Profiling Violent Crimes. 4 ed: Sage Publications, 2009. 344 p.

Holt TJ. Situating 1 the problem of cybercrime in a multidisciplinary context. Cybercrime Through an Interdisciplinary Lens 2016;26:1.

Holt TJ, Bossler AM. Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior 2008;30(1):1-25.

Houghton T. Does Positivism really work in the social sciences. E-International Students 2011.

Houtepen JA, Sijtsema JJ, Bogaerts S. From child pornography offending to child sexual abuse: A review of child pornography offender characteristics and risks for cross-over. Aggression and violent behavior 2014;19(5):466-73.

Hussain MA, Elyas T, Nasseef OA. Research paradigms: a slippery slope for fresh researchers. Life Science Journal 2013;10(4):2374-81.

Ieong RS. FORZA–Digital forensics investigation framework that incorporate legal issues. digital investigation 2006;3:29-36.

index mundi. United Arab Emirates Demographics Profile 2017; 2017. Available from: http://www.indexmundi.com/united_arab_emirates/demographics_profile.html. 2017].

Internet Watch Foundation. IWF annual report 2016. London: Author; 2016.

Ivaturi K, Chua C, Janczewski L. Impact of Information Seeking and Warning Frames on Online Deception: A Quasi-Experiment. Journal of Computer Information Systems 2017;57(2):139-47.

Jackson JL, van Eshof P, de Kleuver EE. Offender profiling in the Netherlands: Netherlands Inst. for the Study of Criminality and Law Enforcement, 1994.

Jansen van Rensburg SK. Unwanted attention: The psychological impact of cyberstalking on its survivors. Journal of Psychology in Africa 2017;27(3):273-6.

Johnson RB, Onwuegbuzie AJ. Mixed methods research: A research paradigm whose time has come. Educational researcher 2004;33(7):14-26.

Johnson SA. Child Pornography Users & Child Contact Offenders: Applications for Law Enforcement, Prosecution and Forensic Mental Health. International Journal of Emergency Mental Health and Human Resilience 2015;17(4):666-9.

Kaati L, Shrestha A, Sardella T. Identifying Warning Behaviors of Violent Lone Offenders in Written Communication. Data Mining Workshops (ICDMW), 2016 IEEE 16th International Conference on: IEEE; 2016. p. 1053-60.

Kardos G, Smith C. On writing engineering cases. Proceedings of ASEE National Conference on Engineering Case Studies1979. p. 42-50.

Karie NM, Venter HS. Taxonomy of challenges for digital forensics. Journal of forensic sciences 2015;60(4):885-93.

Karmen A. Crime Victims: An Introduction to Victimology. Cengage Learning; 2012. p. 1-36.

Keppel RD, Walter R. Profiling killers: A revised classification model for understanding sexual murder. International Journal of Offender Therapy and Comparative Criminology 1999;43(4):417-37.

Keppel RD, Weis JG, Brown KM, Welch K. The Jack the Ripper murders: A modus operandi and signature analysis of the 1888–1891 Whitechapel murders. Journal of Investigative Psychology and Offender Profiling 2005;2(1):1-21.

Kirwan G. The Psychology of Cyber Crime: Concepts and Principles: Concepts and Principles: IGI Global, 2011.

Kitchenham BA, Pfleeger SL. Principles of survey research: part 3: constructing a survey instrument. ACM SIGSOFT Software Engineering Notes 2002;27(2):20-4.

Kocsis RN. What Is Criminal Profiling?: Springer, 2006.

Kocsis RN, Palermo GB. Criminal profiling as expert witness evidence: The implications of the profiler validity research. International journal of law and psychiatry 2016;49:55-65.

Kohn M, Eloff MM, Eloff J. Integrated digital forensic process model. Computers and security 2013;38:pp.103-15.

Kothari CR. Research methodology: Methods and techniques: New Age International, 2004.

Kowalski RM, Limber S, Limber SP, Agatston PW. Cyberbullying: Bullying in the digital age: John Wiley & Sons, 2012.

Kowalski RM, Limber SP. Psychological, physical, and academic correlates of cyberbullying and traditional bullying. Journal of Adolescent Health 2013;53(1):S13-S20.

Krone T. A typology of online child pornography offending: Australian Institute of Criminology;, 2004.

Lanning KV. Child molesters: A behavioral analysis. 4th ed2001.

LeCompte MD, Schensul JJ. Designing and conducting ethnographic research: Rowman Altamira, 1999.

Levy Y, Ellis TJ. A guide for novice researchers on experimental and quasiexperimental studies in information systems research. Interdisciplinary Journal of information, knowledge, and management 2011;6:151-61.

Likert R. A technique for the measurement of attitudes. Archives of psychology 1932(140):1-55.

Lilley C, Ball R, Vernon H. The experiences of 11-16 year olds on social networking sites. National Society for the Prevention of Cruelty to Children (NSPCC), United Kingdom 2014.

Lillis D, Becker B, O'Sullivan T, Scanlon M. Current Challenges and Future Research Areas for Digital Forensic Investigation. arXiv preprint arXiv:160403850 2016.

Lincoln YS, Guba EG. Naturalistic inquiry: Sage, 1985.

Livingstone S, Carr J, Byrne J. One in three: Internet governance and children's rights. 2016.

Lowe A. Criminal profiling in the investigative process. The National Legal Eagle 2002;8(1):6.

Lowry PB, Zhang J, Wang CL, Wu T, Siponen M. Understanding and Predicting Cyberstalking in Social Media: Integrating Theoretical Perspectives on Shame, Neutralization, Self-Control, Rational Choice, and Social Learning. 2013.

Magaletta PR, Faust E, Bickart W, McLearen AM. Exploring clinical and personality characteristics of adult male internet-only child pornography offenders. International journal of offender therapy and comparative criminology 2014;58(2):137-53.

Malamuth N, Linz D, Weber R. The Internet and Aggression: Motivation, Disinhibitory, and Opportunity Aspects. In: Amichai-Hamburger Y, editor. The social net: Understanding our online behavior

: Oxford University Press; 2013. p. 120-40.

Maple C, Short E, Brown A. Cyberstalking in the United Kingdom: An analysis of the ECHO pilot survey. University of Bedfordshire; 2011.

Martini B, Choo K-KR. Distributed filesystem forensics: XtreemFS as a case study. Digital Investigation 2014;11(4):295-313.

Marziale L, Richard GG, Roussev V. Massive threading: Using GPUs to increase the performance of digital forensics tools. digital investigation 2007;4:73-81.

McEvoy P, Richards D. A critical realist rationale for using a combination of quantitative and qualitative methods. Journal of Research in Nursing 2006;11(1):66-78.

McFarlane L, Bocij P. An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers2003.

McGuire M, Dowling S. Cyber crime: A review of the evidence. Summary of key findings and implications Home Office Research report 2013;75.

Merdian HL, Curtis C, Thakker J, Wilson N, Boer DP. The three dimensions of online child pornography offending. Journal of sexual aggression 2013;19(1):121-32.

Miller L. Serial killers: I. Subtypes, patterns, and motives. Aggression and violent behavior 2014;19(1):1-11.

Mir SS, Shoaib U, Sarfraz MS. Analysis of Digital Forensic Investigation Models. International Journal of Computer Science and Information Security 2016;14(11):292.

Mohtasebi S, Dehghantanha A, Broujerdi HG. Smartphone forensics: a case study with Nokia E5-00 mobile phone. International Journal of Digital Information and Wireless Communications (IJDIWC) 2011;1(3):651-5.

Montasari R, Peltola P, Evans D. Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations. International Conference on Global Security, Safety, and Sustainability: Springer; 2015. p. 83-95.

Navarro JN, Marcum CD, Higgins GE, Ricketts ML. Addicted to the Thrill of the Virtual Hunt: Examining the Effects of Internet Addiction on the Cyberstalking Behaviors of Juveniles. Deviant Behavior 2016;37(8):893-903.

Neuman LW. Social research methods: Qualitative and quantitative approaches. 7 ed. Boston2011.

Nirkhi S, Dharaskar RV. Comparative study of authorship identification techniques for cyber forensics analysis. arXiv preprint arXiv:14016118 2013.

Nobles MR, Reyns BW, Fox KA, Fisher BS. Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. Justice Quarterly 2014;31(6):986-1014.

Noblett MG, Pollitt MM, Presley LA. Recovering and examining computer forensic evidence. Forensic Science Communications 2000;2(4):1-13.

O'Leary Z. The essential guide to doing your research project: Sage, 2013.

Oates BJ. Researching information systems and computing: Sage, 2005.

Ofcom. Children and parents: media use and attitudes report. UK2016.

Office for National Statistics. Internet access - Household and individuals: 2017. UK: Author; 2017.

Ogilvie E. Cyberstalking. Trends & Issues in Crime and Criminal Justice 2000(166):1.

Oriwoh E, Jazani D, Epiphaniou G, Sant P. Internet of things forensics: Challenges and approaches. Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on: IEEE; 2013. p. 608-15.

Orlikowski WJ, Baroudi JJ. Studying information technology in organizations: Research approaches and assumptions. Information systems research 1991;2(1):1-28.

Palermo GB, Kocsis RN. Offender profiling: An introduction to the sociopsychological analysis of violent crime: Charles C Thomas Publisher, 2005.

Palmer G. A road map for digital forensics research - report from the first digital forensics research workshop. Utica, New York: Air force research laboratory, Rome research site; 2001. p. 1-48.

Pascual A, Marchini K, Miller S. 2017 Identity Fraud: Securing the Connected Life. US: Javelin; 2017. p. 65.

Patten ML. Understanding research methods: An overview of the essentials: Taylor & Francis, 2017.

Perumal S. Digital forensic model based on Malaysian investigation process. International journal of computer science and network security 2009;9(8):pp.38-44.

Pew Research Center. Online Harassment 2017. 2017. p. 85.

Pinizzotto AJ. Forensic psychology: Criminal personality profiling. Journal of Police Science & Administration 1984(12):32-40.

Potrata B. Rethinking the ethical boundaries of a grounded theory approach. Research Ethics Review 2010;6(4):154-8.

Quayle E, Taylor M. Child pornography and the Internet: Perpetuating a cycle of abuse. Deviant Behavior 2002;23(4):331-61.

Quick D, Choo K-KR. Impacts of increasing volume of digital forensic data: A survey and future research challenges. Digital Investigation 2014;11(4):273-94.

Rapoport RN. Three dilemmas in action research: with special reference to the Tavistock experience. Human relations 1970;23(6):499-513.

Rashid A, Baron A, Rayson P, May-Chahal C, Greenwood P, Walkerdine J. Who am i? analyzing digital personas in cybercrime investigations. Computer 2013;46(4):54-61.

Reith M, Carr C, Gunsch G. An examination of digital forensic models. International journal of digital evidence 2002;1(3):1-28.

Ressler RK, Burgess AW, Douglas JE. Sexual homicide: Patterns and motives: Simon and Schuster, 1988.

Robson C. Real world research: A resource for users of social research methods in applied settings 3rd edition. West Sussex: John Wiley & Sons; 2011.

Rocha A, Scheirer WJ, Forstall CW, Cavalcante T, Theophilo A, Shen B, et al. Authorship attribution for social media forensics. IEEE Transactions on Information Forensics and Security 2017;12(1):5-33.

Rogers M. The role of criminal profiling in the computer forensics process. Computers & Security 2003;22(4):292-8.

Rogers M, Smoak ND, Liu J. Self-reported deviant computer behavior: A big-5, moral choice, and manipulative exploitive behavior analysis. Deviant Behavior 2006;27(3):245-68.

Rogers MK. Psychological profiling as an investigative tool for digital forensics. Digital Forensics: Threatscape and Best Practices 2015:45.

Rogers MK, Seigfried-Spellar KC. Using Internet artifacts to profile a child pornography suspect. Journal of Digital Forensics, Security and Law 2014;9(1):57-66.

Roussev V, Richard III GG. Breaking the performance wall: The case for distributed digital forensics. Proceedings of the 2004 digital forensics research workshop2004.

Sampasa-Kanyinga H, Hamilton HA. Use of social networking sites and risk of cyberbullying victimization: A population-level study of adolescents. Cyberpsychology, Behavior, and Social Networking 2015;18(12):704-10.

Samy GN, Shanmugam B, Maarop N, Magalingam P, Perumal S, Albakri SH. Digital Forensic Challenges in the Cloud Computing Environment. International Conference of Reliable Information and Communication Technology: Springer; 2017. p. 669-76.

Saunders M. Research methods for business students. 7 ed. India: Pearson Education, 2015. 768 p.

Saunders M, Lewis P, Thornhill A. Understanding research philosophies and approaches. Research methods for business students 2009;4:106-35.

Saunders M, Tosey P. The layers of research design. Rapport, Winter 2012;2013:58-9.

Seigfried-Spellar KC. Distinguishing the viewers, downloaders, and exchangers of Internet child pornography by individual differences: Preliminary findings. Digital Investigation 2014;11(4):252-60.

Seto MC, Cantor JM, Blanchard R. Child pornography offenses are a valid diagnostic indicator of pedophilia. Journal of abnormal psychology 2006;115(3):610.

Seto MC, Eke AW. The criminal histories and later offending of child pornography offenders. Sexual abuse: a journal of research and treatment 2005;17(2):201-10.

Shannon-Baker P. Making paradigms meaningful in mixed methods research. Journal of Mixed Methods Research 2016;10(4):319-34.

Shavers B. Placing the suspect behind the keyboard: using digital forensics and investigative techniques to identify cybercrime suspects: Newnes, 2013.

Shaw ED. The role of behavioral research and profiling in malicious cyber insider investigations. Digital Investigation 2006;3(1):20-31.

Shelton J, Eakin J, Hoffer T, Muirhead Y, Owens J. Online child sexual exploitation: an investigative analysis of offender characteristics and offending behavior. Aggression and violent behavior 2016;30:15-23.

Shenton AK. Strategies for ensuring trustworthiness in qualitative research projects. Education for information 2004;22(2):63-75.

Sheridan LP, Grant T. Is cyberstalking different? Psychology, crime & law 2007;13(6):627-40.

Short E, Guppy A, Hart JA, Barnes J. The impact of cyberstalking. Studies in Media and Communication 2015;3(2):23-37.

Silde A, Angelopoulou O. A Digital Forensics Profiling Methodology for the Cyberstalker. Intelligent Networking and Collaborative Systems (INCoS), 2014 International Conference on: IEEE; 2014. p. 445-50.

Silverman D. Doing qualitative research: A practical handbook: SAGE Publications Limited, 2013.

Silverman D. Qualitative research: Sage, 2016.

Smith A. Record shares of Americans now own smartphones, have home broadband. Pew Research Center; 2017.

Smith SS, Shuy RW. Using Language Analysis for Identifying and Assessing Offenders. 2002:16-21.

Snook B, Cullen RM, Bennell C, Taylor PJ, Gendreau P. The criminal profiling illusion what's behind the smoke and mirrors? Criminal Justice and Behavior 2008;35(10):1257-76.

Snook B, Haines A, Taylor PJ, Bennell C. Criminal profiling belief and use: A survey of Canadian police officer opinion. Canadian Journal of Police and Security Services 2007(5):169-79.

Staude-Müller F, Hansen B, Voss M. How stressful is online victimization? Effects of victim's personality and properties of the incident. European Journal of Developmental Psychology 2012;9(2):260-74.

Steinmetz KF. Craft (y) ness An Ethnographic Study of Hacking. British Journal of Criminology 2014:azu061.

Stephenson PR, Walter RD. Toward Cyber Crime Assessment: Cyberstalking. 6th Annual Symposium on Information Assurance (ASIA'11)2011. p. 1.

Strawhun J, Adams N, Huss MT. The assessment of cyberstalking: An expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse. Violence and victims 2013;28(4):715-30.

Stringer ET. Action research: Sage Publications, 2013.

Suler J. The online disinhibition effect. Cyberpsychology & behavior 2004;7(3):321-6.

Sullivan J, Beech A. Are collectors of child abuse images a risk to children. Policing paedophiles on the Internet 2003:11-20.

Tang Q, Linden L, Quarterman JS, Whinston AB. Improving internet security through social information and social comparison: A field quasi-experiment. Weis 2013 2013.

Tashakkori A, Teddlie C. Sage handbook of mixed methods in social & behavioral research: Sage, 2010.

Taylor M. Child pornography and the internet: Challenges and gaps. World Congress Against the Commercial Sexual Exploitation of Children, Yokohama2001. p. 17-20.

Teddlie C, Tashakkori A. Mixed methods research. The Sage handbook of qualitative research 2011:285-300.

Teing Y-Y, Dehghantanha A, Choo K-KR, Yang LT. Forensic investigation of P2P cloud storage services and backbone for IoT networks: BitTorrent Sync as a case study. Computers & Electrical Engineering 2017;58:350-63.

Tonkin M, Pakkanen T, Sirén J, Bennell C, Woodhams J, Burrell A, et al. Using offender crime scene behavior to link stranger sexual assaults: A comparison of three statistical approaches. Journal of Criminal Justice 2017;50:19-28.

Torres AN, Boccaccini MT, Miller HA. Perceptions of the validity and utility of criminal profiling among forensic psychologists and psychiatrists. Professional Psychology: Research and Practice 2006;37(1):51-8.

Tow WN-FH, Dell P, Venable J. Understanding information disclosure behaviour in Australian Facebook users. Journal of Information Technology 2010;25(2):126-36.

Trager J, Brewster J. The effectiveness of psychological profiles. Journal of Police and Criminal Psychology 2001;16(1):20-8.

Turvey B. Deductive criminal profiling: Comparing applied methodologies between inductive and deductive criminal profiling techniques. Knowledge Solutions Library 1998.

Turvey BE. Criminal Profiling: An Introduction to Behavioral Evidence Analysis. 4 ed: Elsevier Science, 2011.

Turvey BE. Forensic victimology: Examining violent crime victims in investigative and legal contexts. 2 ed: Academic Press, 2014. 656 p.

Tzu S. The art of war: Orange Publishing, 2013.

Vahdati S, Yasini N. Factors affecting internet frauds in private sector: A case study in cyberspace surveillance and scam monitoring agency of Iran. Computers in Human Behavior 2015;51:180-7.

Valjarevic A, Venter HS. Harmonised digital forensic investigation process model. Information Security for South Africa. Johannesburg2012. p. pp.1-10.

Van Aken C. The Use of Criminal Profilers in the Prosecution of Serial Killers. Themis: Research Journal of Justice Studies and Forensic Science 2015;3(1):7.

Van Wilsem J. 'Bought it, but never got it'Assessing risk factors for online consumer fraud victimization. European Sociological Review 2011;29(2):168-78.

Vasiu I, Vasiu L. Light My Fire: A Roentgenogram of Cyberstalking Cases. Am J Trial Advoc 2016;40:41.

Venkatesh V, Brown SA, Bala H. Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. MIS quarterly 2013;37(1).

Vincze EA. Challenges in digital forensics. Police Practice and Research 2016;17(2):183-94.

Vrij A, Hope L, Fisher RP. Eliciting reliable information in investigative interviews. Policy Insights from the Behavioral and Brain Sciences 2014;1(1):129-36.

Walker W. The strengths and weaknesses of research designs involving quantitative measures. Journal of research in nursing 2005;10(5):571-82.

Wall DS. Cybercrimes and the Internet. Crime and the Internet 2001:1-17.

Walsh WA, Wolak J, Finkelhor D. Prosecution Dilemmas and Challenges for Child Pornography Crimes: TheThird National Juvenile OnlineVictimization Study (NJOV-3). 2013.

Warikoo A. Proposed methodology for cyber criminal profiling. Information Security Journal: A Global Perspective 2014;23(4-6):172-8.

Webb L, Craissati J, Keen S. Characteristics of Internet child pornography offenders: A comparison with child molesters. Sexual abuse: a journal of research and treatment 2007;19(4):449-65.

Williams M. Virtually criminal: Crime, deviance and regulation online: Routledge, 2006.

Willis B. The advantages and limitations of single case study analysis. E-International Relation Students 2014.

Winder B, Gough B. "I never touched anybody—that's my defence": A qualitative analysis of internet sex offender accounts. Journal of Sexual Aggression 2010;16(2):125-41.

Wolak J, Finkelhor D, Mitchell K. Internet sex crimes against minors: The response of law enforcement: National Center for Missing & Exploited Children Alexandria, VA, 2003.

Wolak J, Finkelhor D, Mitchell K. Child pornography possessors: Trends in offender and case characteristics. Sexual abuse: a journal of research and treatment 2011;23(1):22-42.

Wolak J, Finkelhor D, Mitchell KJ, Ybarra ML. Online "predators" and their victims. American Psychologist 2008;63(2):111-28.

Woodlock D. The abuse of technology in domestic violence and stalking. Violence against women 2017;23(5):584-602.

Wori O. Computer crimes: factors of cybercriminal activities. International Journal of Advanced Computer Science and Information Technology 2014;3(1):pp. 51-67.

Worsley JD, Wheatcroft JM, Short E, Corcoran R. Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses. SAGE Open 2017;7(2):2158244017710292.

Wortley RK, Smallbone S. Child pornography on the internet: US Department of Justice, Office of Community Oriented Policing Services, 2006.

Yang H, Tate M. A descriptive literature review and classification of cloud computing research. Communications of the Association for Information Systems 2012;31(2):35-60.

Zainal Z. Case study as a research method. Jurnal Kemanusiaan 2007;9.

Zona MA, Sharma KK, Lane J. A comparative study of erotomanic and obsessional subjects in a forensic sample. Journal of forensic sciences 1993;38(4):894-903.

APPENDIX 1: THE ONLINE QUESTIONNAIRE

Behavioural Evidence Analysis in Digital Investigations

Participant Information Sheet

ID 111

A study to investigate the utility of Behavioural Evidence Analysis in the processing of digital evidence in child pornography and cyberstalking cases.

My name is Noora Al Mutawa, a PhD student at the University of Central Lancashire, Preston, UK. I would like to invite you to take part in a research study that aims to examine the extent to which analysing offender and victim behaviours based on the related digital forensic evidence recovered from their digital devices is currently used by practitioners in child pornography and cyberstalking cases. It also aims to examine the perceived utility and associated challenges of using these strategies. The findings from this research will hopefully contribute to further development of knowledge and practice for both public and private sector organisations in order to improve the efficiency of digital forensic investigation processes.

It will be highly appreciated if you could kindly support me in my research work by sharing your valued opinions. If you agree to participate, you will be required to complete a questionnaire that will take approximately (10) minutes. The questionnaire is anonymous and all data is confidential. It will be stored securely in accordance with the Data Protection requirements of the institution, and only myself, my supervisory team and others with legitimate academic need will have access to it.

Taking part in the study is voluntary. You can withdraw your participation at any point until you have clicked the 'submit data' button by closing your browser window and your responses will not be collected. However, please note that once you have submitted the data, it will not be possible to withdraw from the study as all responses are anonymous. Please note that by submitting your answers you indicate consent to take part in this study.

The data from the study will be analysed and the results presented in my Doctoral thesis. It may also be used to write journal articles and conference papers, as well as for teaching purposes. The study is conducted in full accordance with the appropriate ethical rules of the University of Central Lancashire.

If you have any questions or require further information, please do not hesitate to email me, or my supervisor using the contact details below.

Noora Al Mutawa
Email: nal-mutawa@uclan.ac.uk

Supervisor: Dr. Joanne Bryce
Email: JBryce@uclan.ac.uk

University of Central Lancashire,
Preston,
Lancashire
PR1 2HE

Demographics

ID 3

1. What is your gender?

- Male
- Female

ID 6

2. What is your age?

20-30	31-40	41-50	51-60	60+
○	○	○	○	○

7

3. What is your highest education level?

- High school diploma
- Bachelors degree
- Forensic professional certificate
- Police training
- Other - Write In

8

4. What is the area of your primary qualification?

- Computer science/IT-related
- Criminal justice related
- Behavioural science
- Digital forensics
- Other - Write In

9

5. What kind of training related to digital forensics have you undertaken?

ID 10

6. In which country do you currently practice digital forensics?

Option 1
Option 2
Afghanistan
Albania
Algeria
Andorra
Angola
Antigua and Barbuda
Argentina
Armenia
Australia
Austria
Azerbaijan
Bahamas, The
Bahrain
Bangladesh
Barbados
Belarus
Belgium
Belize
Benin
Bhutan
Bolivia
Bosnia and Herzegovina
Botswana
Brazil
Brunei
Bulgaria
Burkina Faso
Burundi
Cambodia
Cameroon
Canada
Cape Verde
Central African Republic
Chad
Chile
China
Colombia

Comoros
Congo, Democratic Republic of the
Congo, Republic of the
Costa Rica
Cote d'Ivoire
Croatia
Cuba
Curacao
Cyprus
Czech Republic
Denmark
Djibouti
Dominica
Dominican Republic
East Timor (see Timor-Leste)
Ecuador
Egypt
El Salvador
Equatorial Guinea
Eritrea
Estonia
Ethiopia
Fiji
Finland
France
Gabon
Gambia, The
Georgia
Germany
Ghana
Greece
Grenada
Guatemala
Guinea
Guinea-Bissau
Guyana
Haiti
Holy See
Honduras
Hong Kong
Hungary
Iceland
India

Indonesia
Iran
Iraq
Ireland
Israel
Italy
Jamaica
Japan
Jordan
Kazakhstan
Kenya
Kiribati
Kosovo
Kuwait
Kyrgyzstan
Laos
Latvia
Lebanon
Lesotho
Liberia
Libya
Liechtenstein
Lithuania
Luxembourg
Macau
Macedonia
Madagascar
Malawi
Malaysia
Maldives
Mali
Malta
Marshall Islands
Mauritania
Mauritius
Mexico
Micronesia
Moldova
Monaco
Mongolia
Montenegro
Morocco
Mozambique
Myanmar

Namibia
Nauru
Nepal
Netherlands
Netherlands Antilles
New Zealand
Nicaragua
Niger
Nigeria
North Korea
Norway
Oman
Pakistan
Palau
Palestinian Territories
Panama
Papua New Guinea
Paraguay
Peru
Philippines
Poland
Portugal
Qatar
Romania
Russia
Rwanda
Saint Kitts and Nevis
Saint Lucia
Saint Vincent and the Grenadines
Samoa
San Marino
Sao Tome and Principe
Saudi Arabia
Senegal
Serbia
Seychelles
Sierra Leone
Singapore
Slovakia
Slovenia
Solomon Islands
Somalia
South Africa

South Korea
South Sudan
Spain
Sri Lanka
Sudan
Suriname
Swaziland
Sweden
Switzerland
Syria
Taiwan
Tajikistan
Tanzania
Thailand
Timor-Leste
Togo
Tonga
Trinidad and Tobago
Tunisia
Turkey
Turkmenistan
Tuvalu
Uganda
Ukraine
United Arab Emirates
United Kingdom
United States
Uruguay
Uzbekistan
Vanuatu
Venezuela
Vietnam
Yemen
Zambia
Zimbabwe

ID 11

7. In which type of organization are you currently employed?

- Law enforcement
- Private consulting firm
- Other - Write In

(untitled)

ID 12

8. How long have you been practicing in the field?

Less than 2 years	2-7 years	8-14 years	15-20 years	Over 20 years

ID 14

9. How many different forensics departments have you worked in?

ID 15

10. What is your current job title?

ID 16

11. Please give an estimate of how many digital forensics investigations have you performed during your career.

1-10	11-20	21-50	51-100	101-200	201-300	300+
○	○	○	○	○	○	○

ID 18

12. What types of crimes have you investigated? (tick all that apply)

- [ ] Homicide
- [ ] Rape
- [ ] Assault
- [ ] Robbery
- [ ] Fraud
- [ ] Hacking
- [ ] Child pornography
- [ ] Cyberstalking
- [ ] Copyright infringement
- [ ] Software piracy
- [ ] Electronic money laundering
- [ ] Cyber terrorism
- [ ] Other - Write In

ID 20

13. Do you follow any specific digital forensic methodology or protocols when working when conducting digital forensics in a case? (If Yes, please specify. If No, please state why)

- Yes
- No

Comments

Behavioural Evidence Analysis

LOGIC Show/hide trigger exists.

ID 21

14. Do you know what Behavioural Evidence Analysis (BEA) is?

- Yes
- No

LOGIC Hidden unless: Question "Do you know what Behavioural Evidence Analysis (BEA) is?" #14 is one of the following answers ("Yes")

ID 22

15. Are you aware of how the different strategies of BEA (equivocal evidence analysis, victimology, crime scene characteristics, and offender characteristics) can be utilized in a digital forensic investigation?

- Yes
- No

LOGIC Hidden unless: Question "Do you know what Behavioural Evidence Analysis (BEA) is?" #14 is one of the following answers ("Yes")

ID 23

16. Have you ever utilized BEA in a digital forensic investigation?

- Yes
- No

LOGIC Hidden unless: Question "Do you know what Behavioural Evidence Analysis (BEA) is?" #14 is one of the following answers ("Yes")

ID 24

17. If you have any comments or insights regarding the utility of BEA for investigating digital crimes, please describe them here:

Child pornography

LOGIC Show/hide trigger exists.

ID 25

18. Have you ever performed digital forensics investigations on child pornography cases?

- Yes
- No

LOGIC Hidden unless: Question "Have you ever performed digital forensics investigations on child pornography cases?" #18 is one of the following answers ("Yes")

ID 26

19. Please give an estimate of how many digital forensics investigations you have performed on child pornography cases.

1-5	6-10	11-20	21-50	over 50 cases
○	○	○	○	○

LOGIC Hidden unless: Question "Have you ever performed digital forensics investigations on child pornography cases?" #18 is one of the following answers ("Yes")

ID 74

20. Thinking about recent child pornography cases you worked on, how do the following statements apply to you:

	Never	Rarely	Sometimes	Most of the time	Always
a. As a first step, I perform a quick review of the available electronic evidence and consider all the possible interpretations of evidence.	○	○	○	○	○
b. I perform a critical assessment of the hypotheses and conclusions made by other investigators (if any were established).	○	○	○	○	○
c. I look for electronic evidence that reflects the behaviour of the offender in an attempt to understand their motivations.	○	○	○	○	○
d. I look for electronic evidence that indicates how the offender obtained the child pornography material (e.g., through P2P networks, downloaded directly from the Internet, created by the offender, etc.).	○	○	○	○	○
e. I look for electronic evidence that indicates the relationship between the victim and offender (e.g., child/parents, student/teacher, etc.), if relevant.	○	○	○	○	○
f. I perform a timeline analysis in an attempt to reconstruct the probable sequence of the events of the crime.	○	○	○	○	○

(untitled)

LOGIC Hidden unless: Question "Have you ever performed digital forensics investigations on child pornography cases?" #18 is one of the following answers ("Yes")

81

21. Please indicate the extent to which you agree with the following statements:

	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
a. Knowing the suspect's technical skills will help me to determine where to look for digital evidence.					
b. Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about their motivations.					
c. Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about their psychological state					
d. Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the risk they pose for reoffending, involvement in other criminal activity, etc.					
e. Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the circumstances of the crime.					
f. Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the sequence of the crime events.					
g. Interpreting the behaviour of the offender from the electronic evidence would not be useful.					
h. Perform the examination of the electronic evidence based exactly on what is asked in the request letter/terms of					

reference/warrant.					
i. Conducting further analysis on the behaviour of the offender would not be an effective use of time, resources, and effort.					

LOGIC Hidden unless: Question "Have you ever performed digital forensics investigations on child pornography cases?" #18 is one of the following answers ("Yes")

ID 45

22. What challenges do you face during the digital forensic investigation of child pornography cases in terms of the examination of the electronic evidence?

LOGIC Hidden unless: Question "Have you ever performed digital forensics investigations on child pornography cases?" #18 is one of the following answers ("Yes")

ID 46

23. What would you suggest to improve the digital forensic investigation of child pornography cases?

Cyberstalking

LOGIC Show/hide trigger exists.

ID 48

24. Have you ever performed digital forensics investigations on cyberstalking cases?

- Yes
- No

LOGIC Hidden unless: Question "Have you ever performed digital forensics investigations on cyberstalking cases?" #24 is one of the following answers ("Yes")

ID 49

25. Please give an estimate of how many digital forensics investigations on cyberstalking cases have you performed.

1-5	6-10	11-20	21-50	over 50 cases

LOGIC Hidden unless: Question "Have you ever performed digital forensics investigations on cyberstalking cases?" #24 is one of the following answers ("Yes")

ID 91

26. Thinking about recent cyberstalking cases you worked on, how do the following statements apply to you:

	Never	Rarely	Sometimes	Most of the time	Always
a. As a first step, I perform a quick review of the available electronic evidence and consider all the possible interpretations of evidence.	○	○	○	○	○
b. I perform a critical assessment of the hypotheses and conclusions made by other investigators (if any were established).	○	○	○	○	○
c. I look for electronic evidence that reflects the behaviour of the offender in an attempt to understand their motivations.	○	○	○	○	○
d. I look for electronic evidence that indicates the relationship between the victim and offender (e.g., written communication).	○	○	○	○	○
e. If the victim and offender were not already known to each other, I look for electronic evidence that reflects the victim's behaviour that may have put them at risk of victimization (e.g., Web browsing activities).	○	○	○	○	○
f. I perform a timeline analysis in an attempt to reconstruct the probable sequence of the crime events.	○	○	○	○	○

(untitled)

LOGIC Hidden unless: Question "Have you ever performed digital forensics investigations on cyberstalking cases?" #24 is one of the following answers ("Yes")

ID 98

27. Please indicate the extent to which you agree with the following statements:

	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
a. Knowing the suspect's technical skills will help me to know where to look for digital evidence.	○	○	○	○	○
b. Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about their motivations.	○	○	○	○	○
c. Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about their psychological state.	○	○	○	○	○
d. Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the risk they pose for reoffending, involvement in other criminal activity, etc.	○	○	○	○	○
e. Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the circumstances of the crime.	○	○	○	○	○
f. Interpreting the behaviour of the offender from the electronic evidence can provide more knowledge about the sequence of the crime events.	○	○	○	○	○
g. Interpreting the behaviour of the offender from the electronic evidence would not be useful.	○	○	○	○	○
h. Interpreting the behaviour of the victim from the electronic evidence can provide more knowledge about what placed them at risk of victimization.	○	○	○	○	○

i. Perform the examination of the electronic evidence based exactly on what is asked in the request letter/terms of reference/warrant.					
j. Conducting further analysis on the behaviour of the offender would not be an effective use of time, resources, and effort.					

LOGIC Hidden unless: Question "Have you ever performed digital forensics investigations on cyberstalking cases?" #24 is one of the following answers ("Yes")

ID 66

28. What challenges do you face during the digital forensic investigation of cyberstalking cases in terms of the examination of the electronic evidence?

LOGIC Hidden unless: Question "Have you ever performed digital forensics investigations on cyberstalking cases?" #24 is one of the following answers ("Yes")

ID 67

29. What would you suggest to improve the digital forensic investigation of cyberstalking cases?

ID 68

30. Thank you for taking part in this survey. If you have any further suggestions, comments, or thoughts that you would like to share regarding this research please list them here:

Debrief information sheet

ID 1

Thank you for taking the time to participate in this study.
The aim of this research was to examine the extent to which digital forensic practitioners use behavioural analysis of evidence related to offenders and victims when processing digital evidence in cases involving child pornography and cyberstalking. It also investigated the perceived utility of these approaches to enhance the quality of the gathered digital evidence, and associated challenges in performing these analyses. Please be assured that the information you have provided will be strictly confidential and anonymous.
If you have any further questions regarding this study or your participation, please feel free to contact me, or my supervisor using the following contact details:

Noora Al Mutawa
Email: nal-mutawa@uclan.ac.uk

Supervisor
Dr. Joanne Bryce
Email: JBryce@uclan.ac.uk