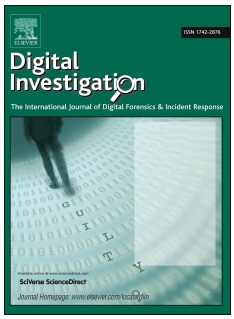
Accepted Manuscript



Behavioural Digital Forensics Model: Embedding Behavioural Evidence Analysis into the investigation of digital crimes

Noora Al Mutawa, Joanne Bryce, Virginia N.L. Franqueira, Andrew Marrington, Janet C. Read

PII: S1742-2876(18)30198-1

DOI: https://doi.org/10.1016/j.diin.2018.12.003

Reference: DIIN 800

To appear in: *Digital Investigation*

Received Date: 25 April 2018

Revised Date: 7 November 2018

Accepted Date: 12 December 2018

Please cite this article as: Al Mutawa N, Bryce J, Franqueira VNL, Marrington A, Read JC, Behavioural Digital Forensics Model: Embedding Behavioural Evidence Analysis into the investigation of digital crimes, *Digital Investigation* (2019), doi: https://doi.org/10.1016/j.diin.2018.12.003.

Behavioural Digital Forensics Model: Embedding Behavioural Evidence Analysis into the Investigation of Digital Crimes

Noora Al Mutawa[a,b], Joanne Bryce[c], Virginia N. L. Franqueira[d], Andrew Marrington[e], Janet C. Read[f]

[a]*School of Computer Engineering and Physical Sciences, University of Central Lancashire, Preston, UK*
[b]*General Department of Forensic Sciences and Criminology, Dubai Police G.H.Q., Dubai, United Arab Emirates*
[c]*School of Psychology, University of Central Lancashire, Preston, UK*
[d]*College of Engineering and Technology, University of Derby, Derby, UK*
[e]College of Technological Innovation, Zayed University, Dubai, UAE
[f]*School of Computer Engineering and Physical Sciences, University of Central Lancashire, Preston, UK*

Abstract

The state-of-the-art and practice show an increased recognition, but limited adoption, of Behavioural Evidence Analysis (BEA) within the Digital Forensics (DF) investigation process. Yet, there is currently no BEA-driven process model and guidelines for DF investigators to follow in order to take advantage of such an approach. This paper proposes the Behavioural Digital Forensics Model to fill this gap. It takes a multidisciplinary approach which incorporates BEA into in-lab investigation of seized devices related to interpersonal cases (i.e., digital crimes involving human interactions between offender(s) and victim(s)). The model was designed based on the application of traditional BEA phases to 35 real cases, and evaluated using 5 real digital crime cases - all from Dubai Police archive. This paper, however, provides details of only one case from this evaluation pool. Compared to the outcome of these cases using a traditional DF investigation process, the new model showed a number of benefits. It allowed a more effective focusing of the investigation, and provided logical directions for identifying the location of further relevant evidence. It also enabled a better understanding and interpretation of victim/offender behaviours (e.g., probable offenders' motivations and modus operandi), which facilitated a more in depth understanding of the dynamics of the specific crime. Finally, in some cases, it enabled the identification of suspect's collaborators, something which was not identified via the traditional investigative process.

Keywords: Behavioural Evidence Analysis; reconstruction of digital crime; digital forensics investigation; behavioural digital forensics model; digital evidence interpretation.

1. Introduction

The utility of Behavioural Evidence Analysis (BEA) has gained attention in the field of Digital Forensics (DF) in recent years (Casey, 2011b, Rogers, 2015, Rogers and Seigfried-Spellar, 2014, Silde and Angelopoulou, 2014, Turvey, 2011a). It has been recognised that in some types of digital crime, along with the technical examination of digital evidence, it is beneficial for the investigation to examine behavioural clues related to offender/victim activities present in the digital evidence (Casey, 2011b, Rogers, 2015, Turvey, 2011a). This can assist the investigator[1] in producing a better justified and more coherent reconstruction of the crime, in interpreting associated digital evidence, and in the

[1] The terms "investigator" and "practitioner" are used interchangeably to refer to the person conducting the DF investigation on the seized digital devices for a case.

description of investigative findings (Al Mutawa et al., 2015, 2016).

Previous studies have demonstrated that BEA has applicability and utility when integrated within the DF investigation process in a post-mortem examination, analysis, and interpretation of the digital evidence for specific types of digital crimes (Al Mutawa et al., 2015, 2016). These benefits include focusing and speeding up the investigation, inferring victim/offender behaviour, inferring offender motivation, identifying potential victims, and eliminating suspects.

Despite the identified utility of BEA, there is no DF process model that provides clear, explicit, and comprehensive steps for "how" it can be performed within the DF investigation process. The available literature only provides a general explanation of the strategies of BEA, and its claimed utility in investigating digital crimes (Rogers, 2003, Rogers, 2015, Turvey, 2011a).

This paper aims to address this identified gap in the literature in three ways. Firstly, it focuses on integrating BEA within the DF investigation process during the in-lab examination, analysis, and interpretation of the data contained within digital devices associated with the case under investigation. The multidisciplinary approach of this work will advance DF state-of-practice by incorporating the stages of BEA into current DF process models to develop a new framework which provides more specific detail about the required strategies in each phase. Secondly, it employs an empirical methodology to develop the proposed model based on two empirical studies that examined the utility and applicability of BEA on thirty five real digital crime cases related to cyberstalking and the possession and dissemination of Indecent Images of Children (IIOC), obtained from the Dubai Police (Al Mutawa et al., 2015, 2016). Finally, it evaluates the proposed model using a case study of a real digital crime case related to online impersonation and defamation. This was selected from a pool of five digital crime cases involving human interactions between offender(s) and victim(s) also used for evaluation, but not explicitly reported in this paper.

The paper is organised as follows: Section 2 provides background information about criminal profiling and the claimed benefits of BEA in investigating digital crimes. Section 3 identifies the general limitations of previously developed DF process models, and critically reviews two specific models that incorporate aspects of BEA. Section 4 describes the methodology used to develop the proposed behavioural DF model, and section 5 describes its design and different phases. Section 6 uses the case study to evaluate it. Sections 7 and 8 discuss the model's benefits and limitations, respectively, and section 9 presents the conclusions**.**

2. Background

This section provides a brief overview of the history of criminal profiling, and how it relates to the development of BEA.

2.1. 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 based on known characteristics of those who have previously committed similar crimes (Kirwan, 2011, Kocsis, 2006). It offers two distinct strategies for creating a subject profile: inductive and deductive approaches. Inductive profiling utilises statistical analysis of behavioural and psychological data from convicted criminals 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). The investigator then uses criminal databases or records related to the defined characteristics to identify a group of potential suspects (Rogers, 2003). Deductive profiling, on the other hand, relates to case-based investigations. It analyses evidence from the case in question, focusing on identifying specific behavioural and personality traits in order to develop a profile of the specific characteristics of the suspect (Turvey, 2011a, Warikoo, 2014).

2.2. Behavioural Evidence Analysis

Behavioural Evidence Analysis (BEA) is a deductive, case-based investigative approach that analyses evidence from a specific case to identify the specific behavioural and personality characteristics of the suspect (Turvey, 2011a). It uses the forensic evidence available for a case to understand and reconstruct the behaviour of a criminal. This approach consists of four types of analysis: equivocal forensic analysis, victimology, identification of crime scene characteristics, and identification of offender characteristics (Turvey, 2011a).

Equivocal forensic analysis refers to the process of conducting a scientific assessment of the case details that includes a thorough examination, analysis, and evaluation of digital evidence, employing critical thinking, reasoning, and logical analysis (Casey and Turvey, 2011, Turvey, 2011a). Victimology refers to the thorough scientific study of victims' characteristics, daily routines and lifestyle that may have contributed to their selection (Casey and Turvey, 2011, Karmen, 2012). Examining crime scene characteristics requires an identification of the unique aspects of the digital crime scene, which can answer questions regarding the case, uncover further evidence, and reflect the offender's behavioural decisions (Turvey, 2011a). In the final stage, offender characteristics are identified based on the results of the preceding stages of the analysis in order to specify the behavioural traits of the suspect (Turvey, 2011a).

2.3. The Role of BEA in Investigating Digital Crimes

Research has recognised that behavioural analysis of digital data can benefit the investigation of certain types of digital crimes by developing a more effective understanding of the individuals involved in the offence (i.e., offenders and victims), as well as the dynamics of the crime (e.g., Colombini et al., 2012, Nirkhi et al., 2012, Rocha et al., 2017). The analysis of this data can also provide investigators with information about offender motivations, and their relationship to the victim (Casey, 2011a, Smith and Shuy, 2002). The use of specific words and the tone of language used in communications can also reveal the psychological state of the offender (e.g., anger, revenge, greed) (Douglas et al., 1986, Kaati et al., 2016). Analysing files from their computer (e.g., Internet history files, recently accessed files, access dates of files, deleted files) can reveal indicators of suspicious activity, as well as signature behaviour and personalised characteristics of the offender (Rogers, 2003). This helps the investigator to develop leads, and determine the location of additional sources of evidence (Turvey, 2011a).

Two previous studies explored the ways in which BEA can be applied to the DF investigation process in IIOC and cyberstalking cases, and identified its additional contribution to these investigations (Al Mutawa et al., 2015, 2016). They forensically analysed real cases obtained from Police archives, applying the four stages of BEA. The studies identified five benefits: (1) providing investigative focus, speed and direction, (2) inferring victim/offender behaviour, (3) inferring offender motivation(s), (4) identifying potential victims, and (5) eliminating suspects. They provided a foundation for customisation of a DF investigation model that incorporates BEA, which is proposed in this paper.

3. Related Work

Dozens of DF process models have been proposed, developed and refined during the last twenty years. A review of eleven popular models developed between 2001 and 2016 (Ademu et al., 2011, Agarwal et al., 2011, Beebe and Clark, 2005, Carrier and Spafford, 2003, Cohen, 2010, Holder et al., 2001, Kohn et al., 2013, Mir et al., 2016, Montasari et al., 2015, Reith et al., 2002, Valjarevic and Venter, 2012) showed that many were single tiered, and focused on the higher levels of the investigative process without providing much detail of their underpinning principles. Several authors of these models have suggested that additional specific steps within each phase (e.g., providing clearer definitions of what constitutes the phase, identifying the objectives of each phase, providing guiding steps on how to conduct each phase) are needed to provide adequate detail in order for them to be useful to the digital forensic investigator (Carrier and Spafford, 2003, Mir et al., 2016, Montasari et al., 2015, Palmer, 2001, Reith et al., 2002).

Another identified limitation of previous models was their lack of consideration of the human behavioural and motivational factors that have relevance for identifying potential evidence during the investigation process. A review of the models suggested that the authors have mainly focused on the technical aspects of the DF investigation process (e.g., data acquisition, preservation of volatile data).

Section 3.1 examines two models that have specifically attempted to integrate BEA within the DF investigation process.

3.1. Integrating BEA in Digital Forensics Investigation Models

Two published models that have incorporated aspects of BEA within the DF investigation of digital crimes are: (1) Digital Forensics Profiling Methodology for Cyberstalkers (Slide & Angelopoulou, 2014), and (2) the Behavioural Analysis Model (Rogers, 2015). Sections 3.1.1 and 3.1.2 review these models respectively.

3.1.1. Digital Forensics Profiling Methodology for Cyberstalkers

Silde and Angelopoulou (2014) developed a cyberstalker profiling methodology which incorporated BEA elements into a standard DF investigation framework. Their model consisted of 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 (e.g., equivocal forensics analysis, victimology). The model also included specific details that described input (e.g., offender skill level, *modus operandi* (MO)) and output (e.g., evidence location, anti-forensics) within each stage.

To evaluate the model, the authors simulated the behaviour of a cyberstalker and a victim. A pre-selected set of behaviours was simulated on two virtual machines that represented both parties. This focused mainly on email communications, instant messaging conversations, social networking activities, some basic anti-forensics techniques, web surfing, and search queries. The investigation focused on identifying the location of evidence on both the victim and the offender's machines. It provided minimum detail about victim or offender behaviour, probably due to the fact that it was tested using a simulation that provided limited offender and victim activities.

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). The authors focused on the technical phase of the methodology by using digital evidence (e.g., use of specific anti-forensics tools, communication files) to guide the search and recovery of evidence. They referred to the use of BEA stages in conducting the investigation, but did not offer any guidelines on how to conduct these stages within the different phases of the methodology. They also touched on offender motivations, MO and skill, yet did not provide sufficient practical guidance on how to establish this information.

The evaluation methodology used in this study was not sufficiently robust to assess the applicability and utility of the proposed model. Since simulation of a predefined set of cyberstalking activities were used, the researchers were already aware of the evidence to look for during the examination and analysis of the victim and offender's machines. As such, this is not fully sufficient to show how using the model, for example, can provide investigative direction. Also, the simulation did not include enough realistic information to illustrate offender characteristics (e.g., motivations, intent), which helps better understand aspects of a case. In summary, they did not use real cases for evaluating their model. Further tests using existing cases and related digital evidence are needed to better evaluate the applicability and utility of the model.

3.1.2. Behavioural Analysis Model

Rogers (2015) argued that DF places greater emphasis on the principles of computer science and engineering (e.g., file carving, hash functions), while paying less attention to traditional investigative approaches. As a result, the investigative process is mainly concerned with data collection, with less focus on its examination and analysis. He proposed a model which incorporated aspects of BEA into the process of DF investigation. This 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, focusing on the statistical analysis and timeline analysis/visualization 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 in order to provide insights into the possible locations of relevant evidence. During the collection phase, the digital investigator works with the behavioural analyst to search for, identify and prepare data relevant to the case in preparation for analysis and interpretation. The statistical analysis phase focuses on conducting frequency analysis on the available data to assist in identifying and interpreting relevant patterns. 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 webpages, times of visits, and types of uploaded/downloaded files. This can then be used to create an online behavioural profile of the user. Timeline analysis/visualization aims to combine the results from the frequency analysis phase with their associated timestamps (e.g., timestamps of downloading specific files, visiting webpages) to visualise usage of the computer. This can further assist the investigation, for example, by associating computer usage at a specific time with a specific individual (in cases where the computer has multiple users). The decision/opinion phase concentrates on

producing the final report, and addresses the questions presented at the start of the investigation. In this phase, the practitioner 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) demonstrated the application and usability of his model by employing three case studies based on real cases from different categories of crimes (i.e., arson, murder, IIOC). However, while the model consisted of six phases, this evaluation focused mainly on the investigative benefits of two phases: (1) frequency analysis, and (2) timeline analysis. Finally, the study did not provide sufficient guidelines that DF investigators can follow while investigating a digital crime.

The review of previous models indicated an increased recognition of the utility of BEA, but reflected a limited adoption of its specific strategies within the DF investigation process. This highlights the need for a more comprehensive BEA-driven model that illustrates and clarifies the steps required in conducting an integrated DF investigation. The next section describes the methodology adopted to develop the model proposed in this paper.

4. Methodology for Design of the Proposed Model

This paper reports the final product of a broader programme of multidisciplinary research that developed a DF model that incorporates BEA strategies. It focused on the post-mortem in-lab examination, analysis, and interpretation of digital evidence associated with digital crimes. The methodology followed is illustrated in Figure 1.

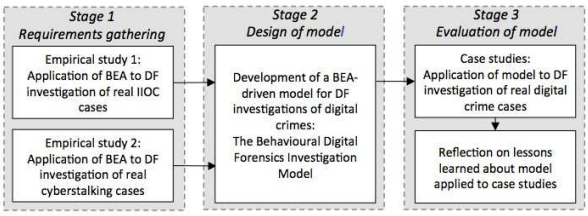


Figure 1. Illustration of the methodology

The process of developing the proposed model involved three main stages. Stage 1 (Figure 1) constituted of two empirical studies that employed a mixed-methods approach with quantitative and qualitative analysis of relevant digital evidence, and case documentation. These studies examined the utility of BEA during the DF process for two types of digital crimes: IIOC (Al Mutawa et al., 2015) and cyberstalking (Al Mutawa et al., 2016). These specific crime categories were selected for a number of reasons. Firstly, there is a relatively small body of empirical research on the behaviour and characteristics of online IIOC 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). Secondly, the investigation and prosecution of IIOC cases requires more than simply locating the abusive imagery on the suspect's digital device. For example, it is necessary to demonstrate (using the available digital evidence) that the suspect was aware of the download of IIOC in order for them to be prosecuted (Akdeniz, 2016, Walsh et al., 2013). The use of technology in the commission of IIOC offences, however, raises significant investigative and evidential challenges (e.g., multiple computer users, the increased use of strategies to evade detection, claims of unintentional download (Balfe et al., 2015, Franqueira et al., 2018, Internet Watch Foundation, 2016, Walsh et al., 2013)). As a result, the theoretical and empirical literature on this offence category 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 BEA have been used to empirically investigate cases of IIOC.

Likewise, the crime category of cyberstalking was selected for the second part of Stage 1 for a number of reasons. The use of advanced technologies to commit this offence also raises specific 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 platforms (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).

Behaviour associated with IIOC and cyberstalking crime categories generates specific forms of evidence which can be extracted from digital devices during the investigative process. This evidence can then be analysed using BEA in order to build a specific profile of offenders to determine the motivations associated with their behaviour, their relationship

with the victim(s), and the interpretation of digital evidence (Al Mutawa et al., 2015, 2016).

The selection of cases utilised criterion sampling (Patton, 2001), with inclusion based on offender behaviour which met the legal definition of IIOC and cyberstalking, use of a computer as the main offending platform, the availability of image files, and the availability of interview scripts with offenders/victims. For each type of crime, a selection of archived cases (15 IIOC and 20 cyberstalking cases) were obtained from the Dubai Police. The crimes were committed in Dubai between 2009 and 2013. Offenders were arrested, however, the police documents did not include information on whether they were subsequently convicted. Since similar technology is used for committing these crimes internationally, it is fair to say that the selected cases would be generalisable to other agencies worldwide. We are not aware of any additional non-technological factors in the selected cases which would make them unique to the UAE or otherwise not generalisable.

Each case was examined and analysed individually using the standard DF procedure (Casey, 2002), and the four strategies of BEA (equivocal evidence analysis, victimology, crime scene characteristics, and offender characteristics). The examination produced qualitative data that was processed using thematic analysis (Braun and Clarke, 2006) (e.g., offender motivations reflected by the digital evidence). All case related documents (e.g., background of offence, interview scripts) were also analysed using descriptive statistics to provide demographic data about offenders and victims, and the involved offending behaviours. The two studies assisted in the development of empirical evidence indicating the usability and utility of incorporating BEA into the investigated cases. It also identified the potential limitations of such an approach.

Along with the review of process models which incorporate BEA reviewed in Section 3.1, this examination helped to 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.

Stage 2 of the model development (Figure 1) focused on design, and incorporated BEA strategies based on input from Stage 1. The final phase, Stage 3 (Figure 1), employed a case study approach to evaluate and illustrate the investigative importance and utility of the model. Five interpersonal crime cases obtained from the Dubai Police archive were used. The selection of cases utilised a criterion sampling (Patton, 2001) with inclusion based on the following criteria: (1) offender behaviour which met the definition of interpersonal crimes, (2) use of a computer as the main offending platform, (3) the availability of image files, and (4) the availability of interview scripts with offenders/victims. The cases were crimes committed in Dubai between 2009 and 2013.

The researchers used the phases and sub-phases of the developed model and described how each of them was conducted in relation to the investigation of each case. A case study strategy (Bryman, 2015, Hancock and Algozzine, 2015) 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. However, only one case study is reported in this paper due to space limitations. This involved impersonation and defamation on Facebook. This specific case was selected as it represents a typical interpersonal digital crime and level of complexity (involving three types of criminal conduct as described later in Section 6.1) without overwhelming the reader with too much detail.

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.

5. The Behavioural Digital Forensics Investigation Model

This section proposes a DF investigation model that incorporates aspects of BEA. 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 digital crimes. The model adheres to commonly used DF process principles (i.e., confidentiality, integrity, and availability) (Ieong, 2006).

The proposed four-stage model was designed using a high-level categorisation in order to enable generalisation across different types of digital interpersonal crimes. It is presented in a linear format in order to provide a clear overview of the phases and sub-phases of the investigation. However, in practice, the investigative process is dynamic and iterative. New evidence about the victim, offender, and offending process can appear throughout the course

of an investigation. This can raise new questions, and require 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 BEA on real IIOC and cyberstalking cases, as mentioned in Section 4. The phases and sub-phases of the model were also derived from Roger's behavioural analysis model (2015), and the DF profiling methodology for cyberstalking proposed by Silde and Angelopoulou (2014) reviewed in Section 3.1. These models were selected because they encompass relevant aspects of BEA, though they are not necessarily explicitly described.

The model does not describe the acquisition and validation of the content of the seized electronic devices. This process is already well developed, with practical guidelines available (e.g., ACPO guidelines in the UK (Williams, 2012)), therefore, it is deemed not relevant to the BEA-driven model. For the sake of the discussion, it is assumed that that forensically-sound images of electronic devices have already been acquired.

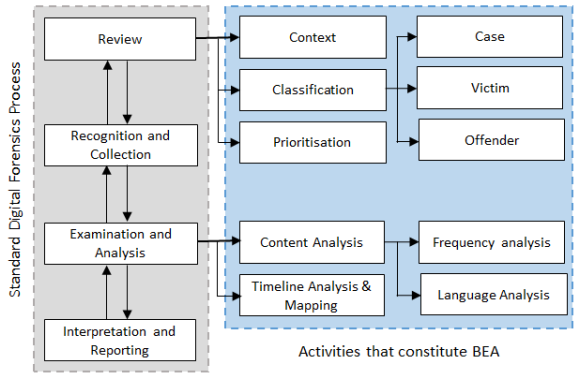


Figure 2. The Behavioural Digital Forensics Investigation Model

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

Sections 5.1-5.4 provide a discussion of the primary phases and the sub-phases of the proposed model, and describe the key tasks in each phase.

5.1. Phase 1: Review

The initial phase is derived from the *Threshold Assessment* process described by Turvey (2011b). This involves a review of the currently available evidence and the established case facts relevant to the crime related behaviour and victimology. It also examines potential offender motivations, behaviour and characteristics, as well as crime scene characteristics. It aims to provide immediate investigative direction, and assist the investigator to develop an initial overview of the case and the involved parties. It also aims to draw initial insights into the offender's risk in order to take immediate actions if required. It does not involve a full analysis of the case-related digital devices. 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 5.1.1-5.1.3.

5.1.1. 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 specific offender characteristics (e.g., history of assaultive behaviour, criminal record, and psychiatric history) should also be identified and included. This can assist the investigator to determine offender risk (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 (Casey, 2011a).

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 offender and/or victim statements.

All assumptions and interpretations from other practitioners 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 (Casey and Turvey, 2011). It also provides them with an initial profile of the offender which can inform the later stages of the investigation (Casey and Turvey, 2011).

5.1.2. 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 case category and determine its initial level of complexity. Different types of cases (e.g., IIOC, cyberstalking, fraud, extortion) have unique characteristics and dynamics. However, cases within the same crime category also 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 is further informed by the *prioritisation* sub-phase discussed in Section 5.1.3.

Building a preliminary profile of the victim (forensic victimology) is also an important step in answering case questions. This process involves the use of a scientific method to examine and interpret specific victim related evidence in order to answer investigative questions (Turvey and Freeman, 2011). It also assesses *victim exposure* (risk assessment), examining how specific factors may have contributed/increased the victim's contact with the offender and subsequent harm (Casey, 2011a, Turvey and Freeman, 2011). The profile includes information such as the victim's demographics, technical skills and physical characteristics, as well as their lifestyle and behavioural characteristics. This assessment enables the investigator to determine factors which provided opportunities for victimisation, and to identify the relationship between the victim and the offender (Casey, 2011a). 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 loopholes, and do not provide a complete picture of the incident (Fisher et al., 1989, Geiselman and Fisher, 2014). The investigator needs to use evidence gathered from the associated digital devices in order to fill these gaps and develop a more detailed understanding of the incident. They also need to weigh the conflicting and shifting accounts of 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, and 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. Risk assessment instruments (e.g., RAGE-V (Association of Threat Assessment Professionals, 2006), Static-2002 (Hanson and Thornton, 2003)) can also be utilised to gather information on the suspect, and measure the potential risk that they may pose for further offending. The use of such tools can facilitate both inductive and deductive analysis, allowing the investigator to correlate suspect personal traits and characteristics with those of known offenders. The combined inductive and deductive techniques strengthen the results of the analysis, which can further assist the investigation by guiding the case planning. However, these tools should be used with caution, considering the applicability of the specific tool to the case under investigation.

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

5.1.3. 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.

5.2. Phase 2: Recognition 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 recognise 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). A number of emerging techniques that have potential for aiding with author attribution includes keystroke mouse-movement analysis, email behaviour, computer usage behaviour, credit card use, and game strategy (Feher et al., 2012, Gupta and Rogers, 2016, Mondal and Bours, 2016, Yampolskiy and Govindaraju, 2008).

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 recognises evidence files, they should then be collected and sorted in a way that will enable a focused and structured examination and analysis which are the next phase.

5.3. 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 5.3.1 and 5.3.2.

5.3.1. Content Analysis

In digital 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). Their careful examination 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 digital crimes involve the online activities of suspects and victims, it is essential to analyse the different behaviour that are reflected by these activities. For example, in IIOC cases, a frequency analysis of the visited websites, downloaded files, search history, and cache files can provide various investigative leads (Al Mutawa et al., 2015). It can also help the practitioner to identify the periods of high online activities and/or computer usage, frequently visited web sites and downloaded/traded files (Rogers, 2015, Rogers and Seigfried-Spellar, 2014). Furthermore, the volume of indecent images and videos on the suspect's computer, the frequency of IIOC-related search queries and related visited web sites can be of significant investigative utility (Al Mutawa et al., 2015). These factors can provide sufficient evidence that the user intentionally sought out IIOC and exercised control over them (Al Mutawa et al., 2015).

Language analysis involves examining and analysing the content 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 for the investigation. For example, many cyberstalkers express (through written communication) their inner emotions (e.g., rage, love) that led them to cyberstalk their victims (Al Mutawa et al., 2016). This can provide the practitioner with an indication of the motivation behind the offender's behaviour. Using a specific writing style and vocabulary can also be a significant psychological indicators of the emotional state of the offender (Hancock et al., 2013). It can also reflect 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 linguistic errors and the frequent use of specific words or phrases can be linked to a specific suspect. Further, assessing the written dialect can assist in profiling the author in terms of native language, age, gender, and educational level (Chaski, 2012). 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, two practical examples of work on this subject were performed by Shaw (2006) and Grant (2012). Extensive work in this area includes that of McMenamin (2002) and Coulthard et al. (2016). Other emerging methods that have potential to be used for author attribution include keystroke and mouse-movement analysis, computer usage behaviour profiling, email behaviour, online game strategy, and credit card use (Feher et al., 2012, Gupta and Rogers, 2016, Mondal and Bours, 2016, Yampolskiy and Govindaraju, 2008).

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.

5.3.2. Timeline Analysis & Mapping

This sub-phase involves analysing the timestamps associated with the files in question (see Section 5.2) and cross examining them with the timeframe 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, if the timestamp of file creation precedes the timestamp of modification can indicate the user had altered the file. As such, timestamp analysis will be a significant part of the investigation in many cases.

5.3.3. 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 practitioner 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.

6. Evaluation of the Proposed Model

This section presents a case study related to impersonation and defamation on Facebook (from a pool of 5 cases used for the evaluation of the proposed model, as mentioned in Section 4). This case illustrates the application and utility of the model depicted in Figure 2 for the DF processing of evidence. The criteria used for selection of cases are also described in Section 4.

The evaluation follows a report format strictly based on the phases and sub-phases of the proposed model (see Figure 2). Note that the model provides practical steps that DF investigators can apply as

required for the investigation of each specific case. The following is a sample of a report outline based on the proposed DF process model:

- Case background
- Review of case documents
    - Context
    - Classification (includes case, victim(s), offender(s) classifications)
    - Prioritisation of devices to be examined
- Recognition and collection of evidence
- Examinations and analysis performed
    - Content Analysis (includes frequency analysis and language analysis)
    - Timeline Analysis and Mapping
- Findings and interpretations

It is important to note that the researchers did not review the original report that included the results of examination and analysis of the case 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 researchers concluded the case analysis in order to compare the findings. Section 6.1 elaborates on the use of the proposed model.

6.1. Impersonation and Defamation on Facebook case study – (Case Background)

The case involved different 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 main 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 researchers have obscured profanity throughout this section. The remaining of this section provides a walk-through of the investigation using the proposed model.

6.1.1. Phase 1: Review

As illustrated in the DF Behavioural Model (see Figure 2), the first phase has three sub-phases: context, classification, and prioritization.

6.1.1.1. Context

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

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 3 shows the Facebook page in question. Note that all identifying information was blurred by the main researcher to preserve Miss X's anonymity.

Figure 3. 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 (Z City).

College (Country B) country of prostitution and wh@$ing.

High School School of bit@$ing and wh@$ing.

6.1.1.2. Classification

Initially, the incident was categorised as an interpersonal offence that constituted at three types of criminal conduct (see beginning of Section 6.1). 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 this possibility, it was 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 in 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 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.

6.1.1.3. Prioritisation

In order to prioritise the laptops seized, a quick string search was performed on specific locations on each device 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 3) 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).

6.1.2. Phase 2: Recognition 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.

6.1.3. Phase 3: Examination and Analysis

The results indicated 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). Analysis of the timestamps associated with the entries 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.

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 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 content of the emails exchanged during the two month 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 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 were extracted from Miss X's work colleague's 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.

6.1.4. Phase 4: Interpretation and Reporting

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 for 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 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 to perform the misconduct.

The 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 against the content of their statements, and (2) examining Miss X's workstation in order to gathering evidence of the MO of stealing her Facebook login credentials. However, as the case was an archived file, the researcher had to use the available evidence

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. Discussion

The case study demonstrated the benefit of the combined approach of standard DF and BEA in providing interpretative and investigative utility. This section discusses these benefits by comparing the results in the original case files of the sample case to the outcomes of the examination conducted by the main researcher using the proposed model.

For the elaborated case (Section 6), 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

6.1.3 for full details). This 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) directly following the request letter 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, this may have been performed in an ad-hoc manner, and without the investigator 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.

The obvious main differences that can be inferred from the DF investigation performed by the main researcher using the proposed model 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 device to start with. Performing the prioritisation step could have reduced the time and effort spent on the examination and analysis of the devices 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. In comparison, the examination and analysis performed in this study went further to investigate the relationship between other suspects connected to the offence.
3. The use of the model enabled an open-minded/multidisciplinary approach to examination of offender motivations through hypotheses building.

The proposed model is an investigative tool that DF practitioners can utilise for the investigation of interpersonal crime 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 from 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 deceptive answers.

Utilising the proposed model demonstrated similar benefits to the other 4 digital interpersonal crime cases tested in the original research. All of the cases used (i.e., extortion, money forwarding scam, false accusation, and employment scam) included digital evidence that reflected human interactions. It is worth

noting that the proposed model is not intended for the investigation of types of digital crimes which involve limited or no human interaction, for instance, those in which automated tools are used to commit the crime (e.g., malware infection, and denial of service attacks).

8. Limitations

Whilst the proposed model provides a useful tool for the investigation of certain types of digital crimes, it is important to recognise that it is not without limitations. The potential to use the model is influenced by the availability of sufficient case information, and 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 also influence the later phases of the model as well (i.e., Recognition and Collection, Examination and Analysis, and Interpretation and Reporting), resulting in a misguided and/or unfocussed investigation. On the other hand, the behavioural analysis 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 (e.g., 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 behavioural analysis. To derive the greatest benefit from the model, it is essential for the practitioner to be well equipped with the necessary skills and knowledge in both disciplines. The practitioner's critical skills, intuition, and judgment can have a high impact on the application and outcomes of the model. They must utilise their skills and knowledge, and work with caution and objectivity to provide the most appropriate analysis and interpretation of the recovered digital evidence. This indicates the importance of training in the relevant disciplines. However, there is always the possibility of unintentional subjectivity and bias in the practitioner's 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 literally without considering the unique aspects of each case can greatly limit its investigative value.

The previous limitation, however, can be addressed by the use of multidisciplinary investigative 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.

Finally, while the proposed 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 digital interpersonal crimes. Future effort should also be focused on determining whether it is possible to impose minimum educational and training requirements for DF investigators in relation to making them better qualified to employ BEA within the DF investigation process, such as the proposed model. It would also be worth exploring whether the model could be implemented within the larger DF investigation framework.

9. Conclusion

This paper proposed and evaluated a model which combines existing standard practice in the field of DF with strategies of BEA for the technical examination of the digital evidence related to a case. Results showed that using the proposed model when investigating digital crimes of interpersonal nature 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 effectiveness and efficacy of the investigation. It also enabled a better understanding and interpretation of victim/offender behaviours (e.g., probable offender motivations and modus operandi, amount of planning, victim risk factors), which facilitated a more in depth understanding of the dynamics of the specific crime. Finally, in some cases, it enabled the

identification of suspect's collaborators, which was not identified via the traditional investigation.

One implication of this work is the ability to show practically that BEA can be applied and be of use within the DF investigative process for specific categories of digital crimes (i.e., interpersonal crimes). It has been theorised in the past that the different stages of BEA can provide investigative value to the DF investigation (Casey and Turvey, 2011, Rogers, 2015, Turvey, 2011a), however, this had not been tested empirically in previous work. It is hoped that the knowledge gathered in this paper will benefit DF investigators and provide insights on how BEA 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.

Acknowledgements

We thank the Dubai Police for sponsoring one author and their unconditional support for this research.

References

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.

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.

Association of Threat Assessment Professionals. Risk Assessment Guideline Elements for Violence (RAGE-V): Considerations for Assessing the Risk of Future Violent Behavior. Association of Threat Assessment Professionals Sacramento, CA; 2006.

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.

Beebe NL, Clark JG. A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation 2005;2(2):147-67.

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.

Bryce J, Franqueira VN, Marrington A. Special issue on cyberharassment investigation: Advances and trends. Journal of Digital Forensics, Security and Law (JDFSL) 2016.

Bryman A. Social research methods: Oxford university press, 2015.

Carrier B, Spafford EH. Getting physical with the digital investigation process. International journal of digital evidence 2003;2(2):1-20.

Casey E. Handbook of computer crime investigation: forensic tools and technology. 1 ed: Academic press, 2002.

Casey E. Cyberpatterns: Criminal behavior on the Internet. Criminal Profiling: An Introduction to Behavioral Evidence Analysis. 3rd ed: Elsevier Science; 2011a. p. 361-78.

Casey E. Digital evidence and computer crime. 3rd ed: Elsevier, 2011b.

Casey E, Turvey B. Investigative reconstruction with digital evidence. Digital evidence and computer crime. 3rd ed: Elsevier; 2011. p. 255-82.

Chaski CE. Who's at the keyboard? Authorship attribution in digital evidence investigations. International journal of digital evidence 2005;4(1):1-13.

Chaski CE. Best practices and admissibility of forensic author identification. JL & Pol'y 2012;21:333.

Cohen F. Toward a science of digital forensic evidence examination. Advances in Digital Forensics VI 2010:17-35.

Colombini CM, Colella A, Mattiucci M, Castiglione A. Network profiling: Content analysis of users behavior in digital communication channel. International Conference on Availability, Reliability, and Security: Springer; 2012. p. 416-29.

Coulthard M, Johnson A, Wright D. An introduction to forensic linguistics: Language in evidence: Routledge, 2016.

Douglas JE, Ressler RK, Burgess AW, Hartman CR. Criminal profiling from crime scene analysis. Behavioral Sciences & the Law 1986;4(4):401-21.

Feher C, Elovici Y, Moskovitch R, Rokach L, Schclar A. User identity verification via mouse dynamics. Information Sciences 2012;201:19-36.

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.

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.

Geiselman RE, Fisher RP. Interviewing witnesses and victims. Investigative Interviewing: Handbook of Best Practices Toronto: Toronto, ON: Thomson Reuters Publishers 2014.

Grant T. Txt 4n6: Method, consistency, and distinctiveness in the analysis of SMS text messages. JL & Pol'y 2012;21:467.

Guarino A. Digital Forensics as a Big Data Challenge. Isse2013. p. 197-203.

Gupta S, Rogers M. Using Computer Behavior Profiles to Differentiate between Users in a Digital Investigation. 2016.

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.

Hanson RK, Thornton D. Notes on the development of Static-2002 (User Report 2003-01). Ottawa, Ontario, Canada: Solicitor General of Canada, 2003.

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.

Holder EH, Robinson LO, Rose K. Electronic crime scene investigation: an on-the-scene reference for first responders. Washington2001.

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.

Ieong RS. FORZA–Digital forensics investigation framework that incorporate legal issues. digital investigation 2006;3:29-36.

Internet Watch Foundation. IWF annual report 2016. London: Author; 2016.

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.

Karmen A. Crime Victims: An Introduction to Victimology. Cengage Learning; 2012. p. 1-36.

Kirwan G. The Psychology of Cyber Crime: Concepts and Principles: Concepts and Principles: IGI Global, 2011.

Kocsis RN. What Is Criminal Profiling?: Springer, 2006.

Kohn M, Eloff MM, Eloff J. Integrated digital forensic process model. Computers and security 2013;38:pp.103-15.

Lillis D, Becker B, O'Sullivan T, Scanlon M. Current Challenges and Future Research Areas for Digital Forensic Investigation. arXiv preprint arXiv:160403850 2016.

McGuire M, Dowling S. Cyber crime: A review of the evidence. Summary of key findings and implications Home Office Research report 2013;75.

McMenamin GR. Forensic linguistics: Advances in forensic stylistics: CRC press, 2002.

Mir SS, Shoaib U, Sarfraz MS. Analysis of Digital Forensic Investigation Models. International Journal of Computer Science and Information Security 2016;14(11):292.

Mondal S, Bours P. Combining keystroke and mouse dynamics for continuous user authentication and identification. Identity, Security and Behavior Analysis (ISBA), 2016 IEEE International Conference on: IEEE; 2016. p. 1-8.

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.

Nirkhi S, Dharaskar RV. Comparative study of authorship identification techniques for cyber forensics analysis. arXiv preprint arXiv:14016118 2013.

Nirkhi SM, Dharaskar RV, Thakre VM. Analysis of online messages for identity tracing in cybercrime investigation. Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on: IEEE; 2012. p. 300-5.

Noblett MG, Pollitt MM, Presley LA. Recovering and examining computer forensic evidence. Forensic Science Communications 2000;2(4):1-13.

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.

Patton MQ. Qualitative evaluation and research methods. 3 ed: SAGE Publications, inc, 2001.

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.

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 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.

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.

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.

Smith SS, Shuy RW. Using Language Analysis for Identifying and Assessing Offenders. 2002:16-21.

Taylor M. Child pornography and the internet: Challenges and gaps. World Congress Against the Commercial Sexual Exploitation of Children, Yokohama2001. p. 17-20.

Turvey BE. Criminal Profiling: An Introduction to Behavioral Evidence Analysis. 4th ed: Elsevier Science, 2011a.

Turvey BE. An introduction to crime scene analysis. Criminal Profiling: An Introduction to Behavioral Evidence Analysis. 4th ed: Elsevier Science; 2011b. p. 141-58.

Turvey BE, Freeman J. Forensic victimology. Criminal Profiling: An Introduction to Behavioral Evidence Analysis. 4th ed: Elsevier Science; 2011. p. 164-85.

Valjarevic A, Venter HS. Harmonised digital forensic investigation process model. Information Security for South Africa. Johannesburg2012. p. pp.1-10.

Vasiu I, Vasiu L. Light My Fire: A Roentgenogram of Cyberstalking Cases. Am J Trial Advoc 2016;40:41.

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.

Williams J. ACPO Good Practice Guide for Digital Evidence. Metropolitan Police Service, Association of chief police officers, GB 2012.

Wolak J, Finkelhor D, Mitchell KJ, Ybarra ML. Online “predators” and their victims. American Psychologist 2008;63(2):111-28.

Yampolskiy RV, Govindaraju V. Behavioural biometrics: a survey and classification. International Journal of Biometrics 2008;1(1):81-113.