Behavioural Evidence Analysis Applied to Digital Forensics: An Empirical Analysis of Child Pornography Cases using P2P Networks

Noora Al Mutawa, Joanne Bryce
School of Psychology
University of Central Lancashire
Preston, UK
nal-mutawa, jbryce@uclan.ac.uk

Virginia N. L. Franqueira
Dept. of Computing & Mathematics
University of Derby
Derby, UK
v.franqueira@derby.ac.uk

Andrew Marrington
College of Technological Innovation
Zayed University
Dubai, UAE
andrew.marrington@zu.ac.ae

Abstract— **The utility of Behavioural Evidence Analysis (BEA) has gained attention in the field of Digital Forensics in recent years. It has been recognized that, along with technical examination of digital evidence, it is important to learn as much as possible 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 shows limited use of BEA for the investigation of cases of the possession and dissemination of Sexually Exploitative Imagery of Children (SEIC). This paper represents a step towards filling this gap. It reports on the forensic analysis of 15 SEIC cases involving P2P filesharing networks, obtained from the Dubai Police. Results confirmed the predicted benefits and indicate that BEA can assist digital forensic practitioners and prosecutors.**

Index Terms— Behavioural evidence analysis, reconstruction, sexually exploitative imagery of children, digital investigation.

I. INTRODUCTION

Offender profiling is a forensic technique used in criminal investigations for analysing, assessing, and interpreting the physical evidence, the crime scene, the nature of the offence and the way it was committed. 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 [1]. A criminal profile may include physical (e.g., gender, age, background), behavioural and psychological attributes (e.g., psychological disorders, guilt, anger). Criminal profiling offers two separate models for creating a subject profile: inductive and deductive. Inductive profiling utilises statistical analysis of behavioural and psychological data from convicted criminals [2]. It relies on data from criminal databases to identify a generalized behavioural pattern and personality traits of a typical offender in specific kind of cases (e.g., rape, serial homicides) [3]. 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 [3]. Deductive profiling, on the other hand, relates to case-based investigation. 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 [4]. Whichever method is used in criminal profiling, it 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 [5, 6].

Previous studies have attempted to produce offender taxonomies in different cybercriminal domains such as hacking, fraud, online SEIC, and insider cases [13-17]. Applying both behavioural and technical analysis to digital evidence can help investigators reveal information about offenders to identify, assess and manage the risk of harm that they may pose before they have a chance to engage in violent behaviour. In addition to the creation of taxonomies of cybercriminals, a number of empirical studies have analysed behavioural trends in organizational cyberattacks. These studies used inductive approaches [18] and aimed to understand the motivations, personal characteristics, modus operandi, and the psychological state of organizational cyber attackers (e.g., [16, 19]).

The studies mentioned above have contributed to the field of behavioural evidence in digital forensics investigations by utilising inductive approaches to produce cybercriminal taxonomies. However, their use in this field depends on statistics and generalization to create an image of the typical perpetrator in specific types of digital crimes. This generalized approach, however, is of limited investigative use and does not make practical sense given the uniqueness and specificity of digital crimes [3]. There is also very little research or practice in digital crime investigations that incorporates behavioural and motivational analysis, particularly for computer-facilitated interpersonal crimes. There is even less in the literature that examines the utility of BEA in assisting the interpretation of digital evidence in these crimes.

One category of computer-facilitated interpersonal crimes that requires more research is the digital possession and dissemination of Sexually Exploitative Imagery of Children (SEIC) or child pornography. 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 [20]. The use of technology in the commission of SEIC offences also raises significant investigative and evidential challenges (e.g., multiple computer users), and the

theoretical and empirical literature on these criminal activities is still in the early stages of development. To date, none of the existing digital forensics research that has incorporated the strategies and principles of BEA have been used to investigate cases of SEIC. Therefore, the main contribution of this paper is to examine the utility of BEA in investigating criminal cases that involve the possession and dissemination of SEIC through P2P networks, and to increase understanding of the benefits of BEA for the interpretation of digital evidence.

This paper is organized as follows. Section II provides background information on the evolution of criminal profiling and BEA. Section III reviews criminal profiling in SEIC-related crimes. Sections IV and V describe the methodology used in the study and the results obtained, respectively. Section VI discusses the results, and finally Section VII draws conclusions and identifies areas for future work.

II. BACKGROUND

In the 1970s, the Behavioural Science Unit of the FBI started using behavioural analysis at crime scenes in an attempt to construct profiles of offender characteristics [7]. Their efforts resulted in the development of the Holmes Typology, which used the inductive approach to identify the common characteristics of offenders of violent serial homicide. The typology depended on the analysis of the crime scene to characterize offenders into two groups: organized and disorganized [3]. In 1992, David Canter developed a scientific psychological model known as Investigative Psychology to assist investigations, also relying on the inductive approach [8]. Similar to the FBI's model, this approach depended heavily on statistics from offender databases [3]. However, he focused on environmental factors and used a Circle Theory that classified offenders as marauders or commuters. Marauders are described as offenders who commit their criminal behaviour in close proximity to their home, whereas commuters are offenders who commit their criminal activities after travelling a distance away from their home [8]. Both the Holmes Typology and the Investigative Psychology approach were developed based on generalization and statistical analysis derived from criminal databases, which make them of limited use in real criminal investigations [3]. They were also criticized for being culturally biased to some extent and cannot be applied worldwide [4]. Further, the Holmes Typology lacked empirical testing, while the use of the Circle Theory in Investigative Psychology was claimed to be ambiguous [3]. In an attempt to overcome some of the limitations of the Holmes Typology and Investigative Psychology, Turvey [4] developed the Behavioural Evidence Analysis Model (BEA). This is based on the deductive approach. It uses the forensic evidence in a case to understand and reconstruct the behaviour of the criminal. His model consisted of four steps: equivocal forensic analysis, victimology, crime scene characteristics, and offender characteristics [4]. A number of studies have emphasized the effective role of BEA in assisting in conventional criminal investigations (e.g., homicide, sex offences, rape) [9, 10]. Rogers [3] realized that BEA can be of equal effectiveness in assisting in the investigation of computer-facilitated crimes. To efficiently solve this type of crime, it is important to learn as much as possible about the individual behind the offence, as well as the victim and the dynamics of the crime [8]. The digital investigator needs to employ more than technical examination of the digital evidence. For example, in a computer-facilitated interpersonal crime, offender behaviour can be interpreted from their written or spoken language (e.g., emails, documents) [3]. Analysing files on the offender's computer (e.g., Internet history files, recently accessed files, time stamps of files, deleted files) can also reveal indicators of suspicious activity, as well as signature behaviours and psychological characteristics of the offender [3]. This helps the investigator to develop leads, and determine the location of additional sources of evidence [4]. After identifying all the supporting evidence in a case, the investigator 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.

According to Casey [11], an equivocal forensic analysis refers to the process of conducting a scientific assessment of the case evidence that includes a thorough examination, analysis and evaluation of evidence, where the interpretation of the evidence remains open for question. This employs critical thinking, reasoning, and logical analysis, as well as a consideration of all the possible interpretations of the evidence. Victimology refers to the study of victims in criminal investigations, and involves a thorough scientific study of a victim's characteristics, daily routines, and lifestyle behaviour that may have contributed to their selection [12]. Crime scene characteristics refer to the careful examination of the unique dimensions of a digital crime scene. They provide useful investigative information which can answer questions regarding the case, uncover additional evidence, and correlate with the offender's behavioural decisions [4]. The final step is analysing offender characteristics. Combining the three preceding behavioural evidence analysis strategies during a digital crime investigation can help determine the probable demographic, behavioural and personality characteristics of the offender.

III. RELATED WORK

SEIC is a form of offending which involves the production, distribution or possession of any visual depiction of children and young people engaging in sexually explicit activity [21], regardless of whether these materials were produced by mechanical or electronic means [22]. 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 [23].

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. 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 [24, 25]. This has facilitated the proliferation of commercial activities related to SEIC, and been a major contributor to increases in the amount and quality of SEIC circulating online [25].

Studies conducted in different parts of the world indicate that the online dissemination and possession 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 [26]. A report by the Federal Bureau of Investigation (FBI) [27] stated that cybercrimes against children have increased around 2000% between 1996 and 2005. The Internet has largely been credited for this increase [26]. A study 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 [28]. 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 access and dissemination of SEIC [29].

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 are only now entering the criminal justice and treatment systems, greater understanding of their psychological characteristics and motivations is required [25] [20]. 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) [20].

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 [30]. 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 [31]. 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 [32-36]. Also, compared to offenders who commit physical sexual offences against minors, Burke et al. observed that online SEIC offenders were generally better educated, employed, in a relationship, and had no criminal history [32]. The diversity of online SEIC offenders demonstrates that inductive profiling is not productive in these cases.

A number of studies have also examined offender motivations for the online collection and dissemination of SEIC. Foley [37] and Bourke and Hernandez [38] suggested that online SEIC are mostly accessed and collected by child sexual offenders and paedophiles. However, other researchers found that online SEIC offenders access and collect these files to obtain sexual gratification and to meet their deviant sexual interests without committing contact offences against children [39, 40]. Other studies have also identified motivations associated with Internet addiction, avoiding negative life experiences, forming social relationships with offenders who have similar interests, and the satisfaction of collecting a complete series of images [41-43]. Motivational factors also include the use of SEIC as a part of physical sexual offending against children, for financial gain, or out of curiosity [24].

Researchers have also attempted to categorize 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 [23, 31, 44]. Based on these factors, Krone [23] developed a typology to describe SEIC offenders that included nine categories:

1. The **browser** refers to an individual who initially views SEIC accidently and does not communicate with online offenders.
2. The **private fantasy offender** creates SEIC representing their sexual fantasy and has the material for their private use.
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.
4. The **non-secure collector** uses websites and chat rooms that do not employ security restrictions to buy, trade, or download SEIC.
5. The **secure collector** obtains SEIC from secured communities and online groups.
6. The **online groomer** seeks online contact with minors with the intention of forming a relationship which progresses to online or physical sexual contact.
7. The **physical abuser** engages in physical sexual abuse of minors and uses online SEIC to complement or facilitate offending.
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.

The behaviours associated with each of these different categories of offending generate specific forms of digital

evidence which can be recovered from computers and other devices during investigations. This can be examined using BEA 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.

IV. METHODOLOGY

The study was conducted at the Department of Electronic Evidence, Dubai Police. The data that was used in this study were bit-wise images 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 the 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).

The study used a deductive, case-based, approach that analysed individual cases separately and applied the four strategies of BEA (equivocal forensics analysis, victimology, crimes scene characteristic, and offender characteristics) to the examination of each case. It examined digital and qualitative information on the application of BEA to cases involving the possession and dissemination of SEIC through P2P file sharing networks on Windows-based computers.

A. Cases Selection and Sample Size

The researcher used criterion-based sampling [26], with the relevant selection criteria being the use of P2P as a main source to acquire SEIC and the availability of the image files of the seized devices. This strategy enabled quality assurance and the identification of information-rich cases. Multiple sources of data were also obtained to provide saturation and confirmation of the emerging results. All of the image files of the seized devices were copied for each selected case, as well as all of its related documents (e.g., offence background, interview scripts, offender information).

The study sample size was determined by a combination of methodological and practical factors. Cases were analysed and added to the sample until there was no new identification of attributes or variables in relation to the specific dimensions of each of the SEIC offences (e.g., no further identification of different techniques to evade detection) [45]. It also depended on, and was highly constrained by, the available resources. As such, 15 cases were selected.

B. Data Sources

The primary data sources for this study were the electronic data stored on the image files of the seized devices for each case (e.g., documents, images, videos, registry keys, Internet cache and history files, metadata of files). Depending on the case, the image files covered devices that ranged from desktop computers and laptops to smart phones and memory cards. As the study utilised a deductive approach, understanding the context of each case was a crucial step prior to analysing the associated evidence. Thus, for each case, all available documentation was carefully studied before the image files were analysed.

C. Data Collection and Analysis

The data collection and analysis combined the technical skills of digital forensics and the reconstruction skills of BEA. The technical skills were required to find sources and traces of evidence required in digital investigations. The process of analysis of the collected data was circular, iterative and progressive. During the examination and analysis of some cases the researcher needed to revisit steps in light of a more refined understanding of the case. The findings of the analysis for each case were summarized, and similar patterns were grouped together. Tabulation and content analysis were also used where applicable. Additionally, a qualitative analysis of relevant case files was undertaken (e.g., offender interviews).

In this type of crime, the digital forensics practitioner usually receives the suspect's digital devices. The examination and analysis of the devices attempts to reconstruct the suspect's activities in obtaining and sharing SEIC. Therefore, the practitioner aims to answer the questions of what, why, where and how the suspect obtained these files using the basic principles of BEA defined by Turvey [2] in the examination and analysis of the data.

The first part of the analysis focused on identifying the locations of all potential sources of digital evidence in a post-mortem forensic examination of the seized devices in each case. The second part focused on identifying offender characteristics, and understanding offending behaviour.

V. RESULTS

This section describes the results of the analysis.

A. Location of Potential Sources of Evidence

An equivocal forensic analysis of the data, and an examination of the virtual crime scene characteristics, showed that the main source of evidence in this category of crimes was the computer of the offender. In the analysed cases, offenders depended mainly on P2P client software for the download and sharing of SEIC. In 73% of the cases, evidence of deleted SEIC files and/or evidence of uninstalled P2P client software and directories was found on the offender's computer(s).

Offenders used a diverse range of P2P software clients (e.g., Shareaza, uTorrent, eDonkey, eMule, ShareStatic, eDonkey2000, BitTorrent). However, a thorough examination of the virtual crime scenes showed that regardless of the kind of P2P client software used, the most common storage location of evidence of SEIC offences was the Program Files directory and sub-directories. In most of these program directories, a shared folder was created where the downloaded files were stored and shared by default unless the user of the programs had disabled sharing in their P2P client. Also, in many of the programs (e.g., Shareaza) an 'Incomplete' folder was created where chunks of the files still being downloaded were stored and shared until the downloaded was complete. Another location of evidence was the library files of the P2P client software. These files stored

important records of the downloaded files (e.g., location, size, filename, thumbnail of the file). In some cases, user created files revealed valuable evidence as some had changed the default download folder of the P2P program to one that they had created. Determining the sharing settings of the P2P program was also important in this offence category as it potentially demonstrates the offender's intention to distribute the files of interest. In many P2P clients, the downloaded files are shared by default unless the user disables the sharing option, making an intention not to share generally easier to establish than an intention to distribute. This was determined either through a review of the registry[1], or by creating a VMware[2] image of the offender's computer hard disk drive. A review of the registry keys also showed search terms that users had entered into the P2P client software, which could establish criminal intent and behaviour.

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, or even complete "active" SEIC files.

B. Offender Characteristics and Behaviour

Using BEA strategies during examination of the sample cases aided in identifying offender characteristics and understanding associated behaviour. The main findings of the analysis are shown in Table I and Table II. Analysis of victimology was not undertaken as there was no evidence of relations/communications between offenders and victims. Also, the physical crime scene could not be directly analysed as the sample cases were from the archive. However, related details were obtained from the police documentation and incorporated into the results.

As shown in Table I, 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%). 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. Also, none of the offenders had been violent to any extent known to law enforcement. Finally, around two thirds of the arrested offenders (67%) came to the attention of law enforcement through online monitoring of P2P files sharing networks, while one third (33%) were arrested after complaints from individuals outside of law enforcement.

TABLE I. CHARACTERISTICS OF SEIC OFFENDERS.

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 SEIC offence	0/15 (0%)
Prior contact offence with a minor	1/15 (7%)
Prior other nonviolent offences	1/15 (7%)
Prior violent offence	0/15 (0%)
No prior arrests	13/15 (87%)

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 filesharing 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, chat logs, and performing string searches did not reveal evidence that the offenders had participated in online offender networks or communities. 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 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 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 amount that ranged between 501-5000 files. 20% were in possession of between 101-500 files, while 13% were in possession of over 5000 files. Analysis of the directories where SEIC were stored showed that most of the offenders (87%) were not concerned with organizing and sorting their files. In most of the cases, besides storing SEIC files in the P2P share folder, copies of the files were 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

[1] A database in a Windows Operating System that stores information about the hardware, software, configuration settings, user profiles, and other important information about the system.

[2] To create a virtual representation of the suspect's computer to visually examine their system in its native operating state.

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 unsuspicious 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 passwords. Only one offender showed a level of technical sophistication by using encryption on an entire hard-disk drive. He also had a VMware within his other computer, and had set up a server of his own.

TABLE II. OFFENDING BEHAVIOUR.

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	
Viewed SEIC	5/15 (33%)
Downloaded SEIC	15/15 (100%)
Shared SEIC	13/15 (87%)
Produced SEIC	0/15 (0%)
Traded SEIC	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	
Used nested directories	3/15 (20%)
Deleted SEIC files/programs	11/15 (73%)
Used wiping tools	0/15 (0%)
Used encryption	1/15 (7%)
Volume of SEIC	
101-500 files	3/15 (20%)
501-1000 files	5/15 (33%)
1001-5000 files	5/15 (33%)
5000+ files	2/15 (13%)

The interpretive and investigative utility of the digital evidence in cases involving the possession and dissemination of SEIC through P2P filesharing networks is summarised in Table III. This demonstrates the utility of the combined analysis of the different types of digital evidence in this crime category.

TABLE III. A SUMMARY OF THE POTENTIAL INTERPRETATIONS AND INVESTIGATIVE UTILITY OF THE DIGITAL EVIDENCE IN CASES INVOLVING THE POSSESSION AND DISSEMINATION OF SEIC THROUGH P2P FILE SHARING NETWORKS.

Digital Evidence	**Behaviour indicated**	**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 gives 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 files. ▪ Shows the user is sharing the files (either intentionally or unintentionally).	▪ Provides evidence of intentional possession of the SEIC files and/or their dissemination.
Partial files in P2P incomplete folder	▪ The user had searched for and is downloading 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 number of times the websites have been visited): ▪ 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).
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 those	▪ Provides proof that the user had downloaded the files.

	files at a certain time before.	▪ Provides a time frame for the downloading of the files, which can be linked to other evidence depending on each case (e.g., if the user had committed contact sexual offence within the same time frame).
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 intended 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.
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 for (e.g., use of extreme, gross, or violent terms). ▪ Can indicate the gender and age preferences of victims in the images and videos.	▪ Provides proof that the user at least intended to view SEIC. ▪ Adds to the quality of evidence if the searched terms match the content of the downloaded files.
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 the 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 had 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 categorizing 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 organized 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 interests.	▪ Sorting through the different types of paraphilic material and their illegality depending on the jurisdiction (e.g., jurisdictions like the UAE prohibits all paraphilic material, while others like the UK does not).
User's subscription to Web sites 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.

VI. DISCUSSION

The results of the study indicated that integrating BEA in digital investigations can greatly assist the investigator in assessing the reliability of digital evidence and the strength of associated conclusions. This can produce a more detailed reconstruction of evidence that can inform sentencing and prosecution in court. It can also assist in mapping and understanding offending behaviour and the dynamics of offences. For example, the location of SEIC files can indicate offender intentions. Some offenders may claim accidental viewing of SEIC while surfing the Internet [46]. However, digital evidence can contradict this claim if SEIC were found to be saved in user created folders. Sorting and categorising the files can further indicate offender intentions, as well as commitment to their interests through spending time and making an effort to classify the files in a particular manner. 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 reflect the offender interests and intentions in finding, viewing, or downloading these files.

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, however, were stored in nested user-created directories that existed under the suspect's user profile. As such, the retrieved 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. First, the amount of SEIC files was not consistent with the claim of accidental access. Second, evidence showed that the website from which the SEIC were viewed has been visited more than once over a certain period of time. As such, with the correct 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.

The study results suggest that it is not possible to construct a single profile of SEIC offenders, as this does not reflect the dynamic nature of individuals as reflected in the basic principles of BEA. However, the identified offender characteristics and behaviour was consistent with prior inductive studies on the same crime category. For example, the majority of SEIC offenders (87%) did not have any known previous offences, and (80%) consumed other paraphilic materials. This is consistent with previous studies [21][47]. Only one of the offenders was previously arrested for attempting to commit another minor offence, which was similar to the results of the study conducted by Niveau [47].

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 producing or trading SEIC. Further, the majority of offenders 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 attempted to groom minors online. One offender, however, might have attempted to progress to contact sexual offence with a minor by making him watch SEIC video that was stored on his mobile phone.

As such, from a theoretical perspective, offenders share general characteristics such as criminal history and sexual interests. However, when it comes to practically investigating individual cases, each offender had his own way of committing the offence. Therefore, generalization is not an effective approach when it comes to the practical part of investigating a case. Each offence and offender is unique, and must be investigated separately to understand the dynamics, actions, and behaviours surrounding the case.

Digital investigators currently lack a systematic method for justifying the digital evidence that aids them at arriving at their conclusions. Because of lack of this formalization, courts and other decision makers find it extremely hard to assess the reliability of digital evidence and the strength of the conclusions arrived at by the investigator. The combined strategy of applying digital forensics analysis and BEA in the current study can contribute to establishing a method for the investigator to justify why and how certain digital evidence can aid in prosecuting cases of SEIC. The employment of the proposed investigative table (Table III) provides investigators with guidelines that they can use in investigating individual cases within this crime category. It also helps less experienced investigators in handling these crimes and researchers who may be interested in building such profiles further.

VII. Conclusion

Previous studies depended on inductive approaches to understand the offending behaviour of criminals arrested in SEIC offences. This study, however, followed a deductive approach by examining each case separately, applying digital forensic analysis and BEA to understand the behavioural dynamics of offenders in this crime category. The preliminary findings showed that utilizing BEA in computer-facilitated interpersonal crimes can assist in the investigation process in a number of ways. First, it can direct investigators to potential sources of digital evidence on the examined devices that might otherwise be overlooked. It also assists suspect interrogations through understanding specific offender characteristics and behaviours. However, the main outcome of the study was establishing a method for authenticating digital evidence that will aid in prosecuting SEIC cases. Table III 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 utilized in investigating individual cases and understanding the dynamics and behaviour of individual offenders. The interpretation table (Table III) can also be utilised by prosecutors to establish a bridge between the behavioural and technical aspects of digital evidence. This can by enable them to better understand the utility of specific digital evidence in supporting the prosecution of SEIC crimes.

As future work, we intend to perform similar studies for other types of computer-facilitated interpersonal crimes (e.g., cyberstalking), and design process models specific to each one incorporating BEA. The aim is to better equip digital forensic practitioners and prosecutors to take advantage of behavioural interpretation of evidence.

Acknowledgment

We thank Dubai Police General Headquarter for providing unconditional educational funding, and for their continuous support for the conduct of this research.

REFERENCES

[1] R. N. Kocsis, *What Is Criminal Profiling?*: Springer, 2006, pp. 1-11, doi: 10.1007/978-1-59745-109-3_1.

[2] B. Turvey, "Deductive criminal profiling: Comparing applied methodologies between inductive and deductive criminal profiling techniques," *Knowledge Solutions Library*, 1998.

[3] M. Rogers, "The role of criminal profiling in the computer forensics process," *Computers & Security*, vol. 22, pp. 292-298, 2003, doi: 10.1016/s0167-4048(03)00405-x.

[4] B. E. Turvey, *Criminal Profiling: An Introduction to Behavioral Evidence Analysis*, 4 ed.: Elsevier Science, 2011.

[5] J. E. Douglas, R. K. Ressler, A. W. Burgess, and C. R. Hartman, "Criminal profiling from crime scene analysis," *Behavioral Sciences & the Law*, vol. 4, pp. 401-421, 1986, doi: 10.1002/bsl.2370040405.

[6] C. Ferguson, "Investigative relevance," in *Profiling and Serial Crime: Theoretical and Practical Issues*, W. Petherick, Ed., 3 ed: Anderson publishing, 2014.

[7] R. K. Ressler, A. W. Burgess, and J. E. Douglas, *Sexual homicide: Patterns and motives*: Simon and Schuster, 1988.

[8] D. Canter and D. Youngs, *Investigative psychology: Offender profiling and the analysis of criminal action*: John Wiley & Sons, 2009, doi: 10.1002/jip.115.

[9] A. Lowe, "Criminal profiling in the investigative process," *The National Legal Eagle*, vol. 8, 2002.

[10] W. W. Bennett and K. M. Hess, "Investigating violent crimes," in *Criminal investigation*, ed: Cengage Learning, 2007, pp. 296-313.

[11] E. Casey, "Investigative reconstruction with digital evidence," in *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, E. Casey and B. E. Turvey, Eds., ed: Academic Press, 2011, pp. 255-273.

[12] A. Karmen, "Crime Victims: An Introduction to Victimology," ed: Cengage Learning, 2012, pp. 1-36.

[13] H. Hayes and T. Prenzler, "Profiling fraudsters," *Final report to crime prevention Queensland*, 2003.

[14] M. R. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, and A. Moore, "Insider threat study: Illicit cyber activity in the banking and finance sector," DTIC Document2004.

[15] M. M. Ferraro and E. Casey, "Investigating child exploitation and pornography: The internet, law and forensic science," ed: Elsevier Academic Press, 2005, pp. 41-74.

[16] M. Keeney and E. Kowalski, "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. 2005," *CERT/CC: Philadelphia, PA*, 2005.

[17] M. K. Rogers, "A two-dimensional circumplex approach to the development of a hacker taxonomy," *Digital Investigation*, vol. 3, pp. 97-102, 2006, doi: 10.1016/j.diin.2006.03.001.

[18] J. Kaarbo and R. K. Beasley, "A Practical Guide to the Comparative Case Study Method in Political Psychology," *Political Psychology*, vol. 20, pp. 369-391, 1999, doi: 10.1111/0162-895x.00149.

[19] E. D. Shaw and L. F. Fischer, "Ten tales of betrayal: The threat to corporate infrastructure by information technology insiders analysis and observations," DTIC Document2005.

[20] J. Wolak, D. Finkelhor, K. J. Mitchell, and M. L. Ybarra, "Online "predators" and their victims," *American Psychologist*, vol. 63, pp. 111-128, 2008, doi: 10.1037/0003-066x.63.2.111.

[21] J. Clough, *Principles of cybercrime*: Cambridge University Press, 2009, doi: 10.1017/cbo9780511845123

[22] P. Jenkins, *Beyond tolerance: Child pornography on the Internet*: NYU Press, 2003.

[23] T. Krone, *A typology of online child pornography offending*: Australian Institute of Criminology, 2004.

[24] A. R. Beech, I. A. Elliott, A. Birgden, and D. Findlater, "The internet and child sexual offending: A criminological review," *Aggression and violent behavior*, vol. 13, pp. 216-228, 2008, doi: 10.1016/j.avb.2008.03.007.

[25] R. K. Wortley and S. Smallbone, *Child pornography on the internet*: US Department of Justice, Office of Community Oriented Policing Services, 2006.

[26] P. Carnes, *In the shadows of the net: Breaking free of compulsive online sexual behavior*: Hazelden Publishing, 2013.

[27] "The Federal Bureau of Investigation's Efforts to Combat Crimes Against Children " Office of the Inspector General, 2009.

[28] R. Cafe, "Police detection of child porn images increases by 48%," in *BBC News*, 2013.

[29] "Database of Electronic Crimes," ed. Dubai - United Arab Emirates: Dubai Police, 2014.

[30] J. Wolak, D. Finkelhor, and K. Mitchell, *Internet sex crimes against minors: The response of law enforcement*: National Center for Missing & Exploited Children Alexandria, VA, 2003.

[31] L. Webb, J. Craissati, and S. Keen, "Characteristics of Internet child pornography offenders: A comparison with child molesters," *Sexual abuse: a*

journal of research and treatment, vol. 19, pp. 449-465, 2007, doi: 10.1177/107906320701900408.

[32] A. Burke, S. Sowerbutts, B. Blundell, and M. Sherry, "Child pornography and the Internet: Policing and treatment issues," *Psychiatry, Psychology and Law*, vol. 9, pp. 79-84, 2002, 10.1375/132187102760196925.

[33] N. Galbreath, F. Berlin, and D. Sawyer, "Paraphilias and the Internet," *Sex and the Internet: A guidebook for clinicians*, pp. 187-205, 2002.

[34] K. C. Seigfried-Spellar, "Distinguishing the viewers, downloaders, and exchangers of Internet child pornography by individual differences: Preliminary findings," *Digital Investigation*, vol. 11, pp. 252-260, 2014, doi: 10.1016/j.diin.2014.07.003.

[35] M. C. Seto and A. W. Eke, "The criminal histories and later offending of child pornography offenders," *Sexual abuse: a journal of research and treatment*, vol. 17, pp. 201-210, 2005, doi: 10.1177/107906320501700209.

[36] J. Wolak, D. Finkelhor, and K. Mitchell, "Child pornography possessors: Trends in offender and case characteristics," *Sexual abuse: a journal of research and treatment*, vol. 23, pp. 22-42, 2011, doi: 10.1177/1079063210372143.

[37] T. P. Foley, "Forensic assessment of Internet child pornography offenders," *The sex offender: Current treatment modalities and systems issues*, vol. 4, pp. 1-18, 2002.

[38] M. L. Bourke and A. E. Hernandez, "The 'Butner Study'redux: A report of the incidence of hands-on child victimization by child pornography offenders," *Journal of Family Violence*, vol. 24, pp. 183-191, 2009, doi: 10.1007/s10896-008-9219-y.

[39] E. Quayle and M. Taylor, "Child pornography and the Internet: Perpetuating a cycle of abuse," *Deviant Behavior*, vol. 23, pp. 331-361, 2002, doi: 10.1080/01639620290086413.

[40] M. C. Seto, J. M. Cantor, and R. Blanchard, "Child pornography offenses are a valid diagnostic indicator of pedophilia," *Journal of Abnormal Psychology*, vol. 115, p. 610, 2006, doi: 10.1037/e674092007-009.

[41] O. Henry, R. Mandeville-Norden, E. Hayes, and V. Egan, "Do internet-based sexual offenders reduce to normal, inadequate and deviant groups?," *Journal of Sexual Aggression*, vol. 16, pp. 33-46, 2010, doi: 10.1080/13552600903454132.

[42] M. C. Seto, L. Reeves, and S. Jung, "Explanations given by child pornography offenders for their crimes," *Journal of Sexual Aggression*, vol. 16, pp. 169-180, 2010, doi: 10.1080/13552600903572396.

[43] B. Surjadi, R. Bullens, J. van Horn, and S. Bogaerts, "Internet offending: Sexual and non-sexual functions within a Dutch sample," *Journal of sexual aggression*, vol. 16, pp. 47-58, 2010, doi: 10.1080/13552600903470054.

[44] E. M. Alexy, A. W. Burgess, and T. Baker, "Internet offenders traders, travelers, and combination trader-travelers," *Journal of Interpersonal Violence*, vol. 20, pp. 804-812, 2005, doi: 10.1177/0886260505276091.

[45] B. G. Glaser, & A. L. Strauss, *The discovery of grounded theory: Strategies for qualitative research*: Transaction Publishers, 2009.

[46] B. Winder, & B. Gough, "I never touched anybody—that's my defence": A qualitative analysis of internet sex offender accounts. *Journal of sexual aggression*, *16*(2), pp. 125-141, 2010, doi:10.1080/13552600903503383.

[47] G. Niveau, "Cyber-pedocriminality: Characteristics of a sample of internet child pornography offenders". *Child abuse & neglect*, *34*(8), pp. 570-575, 2010, doi: 10.1016/j.chiabu.2010.01.011.