Investigation of indecent images of children cases: Challenges and suggestions collected from the trenches.

Investigation of Indecent Images of Children Cases: Challenges and Suggestions Collected from the Trenches

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

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

Abstract

Previous studies examining the investigative challenges and needs of Digital Forensic (DF) practitioners have typically taken a sector-wide focus. This paper presents the results of a survey which collected text-rich comments about the challenges experienced and related suggestions for improvement in the investigation of Indecent Images of Children (IIOC) cases. The comments were provided by 153 international DF practitioners (28.1% survey response rate) and were processed using Thematic Analysis. This resulted in the identification of 4 IIOC-specific challenge themes, and 6 DF-generic challenges which directly affect IIOC. The paper discusses these identified challenges from a practitioner perspective, and outlines their suggestions for addressing them.

Keywords: Indecent Images of Children (IIOC), Sexually Exploitative Imagery of Children (SEIC), Survey, Practitioners Perception, Digital Forensics, Digital Investigation, Child Pornography.

1. Introduction

Possession, production, distribution, and/or publication of Indecent Images of Children (IIOC), also referred to as Sexually Exploitative Imagery of Children (SEIC) or Child Pornography (CP), is a crime in the UK [1] and around the World (e.g., [2]). They are a form of child sexual exploitation which depict children being sexually abused [3].

Technological advances in recent years (e.g., cloud storage, social media, mechanisms for anonymisation, encryption, and P2P communication) have facilitated this type of crime [4, 5]. As a consequence, there has been a sharp increase in indecent image-related offences worldwide [6, 7, 8, 9, 10]. This has put pressure on law enforcement to forensically investigate an overwhelming number of cases, ultimately resulting in offenders being charged and victims safeguarded [11].

This paper reports on the analysis of free-text comments collected via an online survey among Digital Forensics (DF) practitioners[1] dealing with IIOC cases. They were asked to elaborate on the perceived challenges of working in this area, and to suggest relevant solutions and improvements. The contribution of the paper is twofold. First, it adds to the small number of surveys in the DF literature which have examined practitioners' perspectives on the challenges they encounter during their work. Importantly, it also reports on the challenges and suggested solutions for a specific type of case based on 153 respondents working in this area. Second, it takes a multidisciplinary approach to the discussion of the themes identified, adding new perspectives to the challenges and potential solutions which relate to this category of DF investigations.

The paper is organised as follows. Section 2 reviews related survey research examining practi-

*Corresponding author.

[1] The term "DF practitioner" is used in this paper in a broad sense. Therefore, it includes DF roles such as analysts, examiners, investigators, first responders, data recovery engineers, managers, advisors, and consultants. It also includes police officers (e.g., detective inspectors and officers), and unit chiefs currently working in this field.

tioner perspectives on current DF challenges. Section 3 describes the methodology adopted, sample and the related analytic strategy utilised. Section 4 presents the sample demographics and the challenge themes identified. Sections 5 and 6 elaborate on each theme, taking a top-down approach from generics to specifics, respectively. Section 7 discusses practitioner suggestions for addressing the identified challenges. Finally, Section 8 discusses the validity of the study, while Section 9 draws conclusions.

2. Related Work

The related work is organised in terms of the use of surveys and interviews as instruments to examine practitioner perspectives on DF topics.

Rogers et al. [12] analysed the results of a survey with 279 U.S. based law enforcement and prosecutors about their knowledge and willingness to prosecute cases involving digital evidence. This was in the early days of DF, and the study found that digital evidence was not regarded with the same level of importance as physical evidence.

Rogers and Seigfried [13] performed a needs analysis survey and identified top priority issues affecting computer forensics practitioners (i.e., researchers, students, academics, and private/public sector practitioners) based on 60 responses. This resulted in the identification of the following key issues requiring further attention: (1) education/training/certification, (2) technology, (3) encryption, (4) data acquisition, and (5) tools. Harichandran et al. [14] replicated the Rogers and Seigfried [13] survey a decade later with 99 respondents across the following primary occupations: industry instructor, law enforcement practitioner, non-law enforcement practitioner, professor, researcher, and student. Their results aligned with and expanded on these previous findings. They identified the following top needs: (1) better education/training/certification, (2) support for cloud and mobile forensics, (3) backing for and improvement of open source tools, (4) research on encryption, malware, and trail obfuscation, (5) revised laws, (6) better communication with/between law enforcement, and (7) more personnel and funding.

Liles et al. [15] focused on legal aspects affecting DF practice in the U.S. They reported results based on 71 responders from law enforcement, academia, governments, legal/court, and the commercial sector, and found that participants from these different groups disagreed on priorities among legal issues such as international cooperation, interpretation of laws, jurisdictional issues, digital evidence presentation difficulties and the need to test new tools.

Some publications have examined practitioner perspectives on specific aspects of DF. For example, Hibshi et al. [16] investigated factors affecting usability of DF tools using a 2-step approach: interviews with 8 DF practitioners (e.g., law enforcement and industry forensics experts), and a survey with 115 participants at a DF conference. Their findings uncovered a number of usability and technical issues related to commonly used DF tools (e.g. EnCase, FTK, Autopsy and The Sleuth Kit) which can inform the design and implementation of new tools. Ruan et al. [17] reported results from a survey with 257 responders about Cloud Forensics when the term was still ill-defined. The authors claimed that "the participants are experienced, well-educated, and relatively have good knowledge as well as sufficient practical experience in the field of digital forensics" [17, p. 35]. The survey covered respondents' perceptions regarding the definition of the term, significance, impact, challenges, and opportunities for research and development. As a result, a definition of *Cloud Forensics* was proposed, and a list of top challenges derived.

Fahdi et al. [18] investigated DF challenges from the perspective of differences in priority perceived between DF academic researchers and DF practitioners (e.g., law enforcement and organisational). Their survey achieved 42 responses and only identified slight variations in priorities relating to anti-forensics, encryption, Cloud Computing, and social networking between the two groups.

Based on the literature, Amanna and James [19] identified key factors affecting the robustness and resilience of DF laboratories faced with the reality of high staff turnover, complex/changing requirements, and advances in technology. They then conducted a survey examining the current state of robustness and resilience practices among law enforcement agencies and subject-matter experts, receiving responses from 21 practitioners from across the EU. Results revealed that key factors for sustainable DF laboratories spanned across the operational and strategic levels: DF strategy, forensics discipline, standardisation, continuous education and training, research and development, cooperation, and human resources.

These studies demonstrate the utility of survey research with practitioners. They allow us to empir-

ically examine their perspectives on the challenges they face in order to develop a clear evidence base on which to understand their needs, and develop appropriate solutions and responses.

To the best of our knowledge, no published study has addressed the investigative challenges and suggested solutions specifically related to IIOC cases based on practitioners' input. This is important because different categories of offending behaviour, and the related digital forensics evidence they generate, potentially raise challenges which may need crime-specific solutions. This paper contributes towards filling this gap in knowledge and practice.

3. Methodology

The data and analysis reported in this paper is part of a wider dataset collected using an online survey methodology to explore the utility of Behavioural Evidence Analysis (BEA) in investigating IIOC and cyberstalking cases among digital forensics practitioners. It presents the analysis of two free response questions which asked participants to comment on the challenges they faced when performing DF investigations on IIOC cases, and how these could be addressed.

The survey had a total of 30 questions with an anticipated answer time of 10 minutes. All questions were developed by one of the researchers on the basis of their professional experience as a digital forensics investigator. The survey was designed according to best practice recommendations [20, 21]. Potential participants were provided with a briefing and debriefing sheet at the start and end of the questionnaire respectively. This explained the purpose of the study, related participation criteria, and ethical information (e.g., voluntary nature of participation, data anonymity and confidentiality). Completing the survey and submitting the associated data indicated consent to take part in the study.

Only the analysis of the free text comments related to IIOC cases is presented in this paper.

3.1. Procedure & Sample Size

The survey was hosted online for a two month period in 2016. It was promoted by sending invitation emails to potential participants which contained a link to the survey. Participants were mainly recruited through LinkedIn, as well as established connections with national and international DF practitioners. As mentioned in Section 1, the term "DF practitioner" is used in a broad sense in this study; participants were from a variety of DF roles. This included analysts, examiners, investigators, first responders, data recovery engineers, managers, advisors, and consultants, as well as detective inspectors, sargeants, officers, and unit chiefs currently working in the DF field.

Emails soliciting participation were sent to 877 potential participants. A total of 246 respondents completed the survey, resulting on a response rate of 28.1%. However, a closer examination of the survey data showed that 93 entries were incomplete, therefore, they were excluded from the dataset resulting in 153 complete responses being analysed.

3.2. Data Analysis

Thematic analysis [22] was used by the researchers to code the data and identify themes associated with the objectives of the study. The analytic process followed the stages outlined and utilised by other researchers (e.g., [22, 23]), though the data consisted of individual comments made by participants in relation to the survey questions which focused on investigative challenges and improvements. The initial stage of analysis involved the comments in the dataset being read a number of times in order to achieve familiarisation with the data, and to develop a list of coding labels associated which the responses. This was followed by initial coding and organisation of the data [24]. An iterative review process of coding and identification of themes was then undertaken to ensure the accuracy and consistency of the analysis [22]. Illustrative quotations to support the analysis were also identified during this phase.

4. Results

4.1. Demographics

The results of the general demographic questions are presented in Table 1. The sample consisted of a wide range of individuals with varying backgrounds who engage in DF investigations. They came from 36 different countries, with the highest proportion being from the United Kingdom (17.8%) and the United States (16.4%). The majority of the sample were males (88.7%) and 88.7% were aged 31-40 years old. The majority of respondents had a degree qualification at Bachelors (33.7%) or Masters level (25.1%).

	Percentages
Region of Residence	
Europe	40.4
North America	17.1
Middle East & North Africa	16.4
East Asia	11.6
Africa (excluded North Africa)	8.9
Australia/New Zealand	4.7
Gender	
Male	88.7
Female	11.3
Age	
20–30	26.5
31–40	39.7
41–50	18.5
51–60	12.6
Over 60	2.6
Education Level	
High school diploma	5.3
Bachelor's degree	33.7
Master's degree	25.1
PhD degree	3.3
Unspecified	29.8
Training	
DF certificate courses	63.5
Vendor-specific courses	42.0
On-the-job training	10.0
Organisation	
Public sector/Law Enforcement	49.6
Private sector	47.6
Self-employed	1.3
Years of Experience	
Less than 2 years	10.6
2–7 years	37.1
8–14 years	39.1
15–20 years	7.9
Over 20 years	4.6

Table 1: Sample Demographics.

The sample provided a balanced representation of practitioners from the public sector (49.6%) and the private sector (47.6%). 62.2% of participants had digital forensics or cyber security as their primary area of qualification. The majority of participants had more than 2 years of experience: 39.1% reported 8-14 years of practice, while 37.7% reported 2-7 years. 36% of the participants had performed more than 300 DF investigations, and 26.7% had been involved in 101-300 cases. The majority (74.8%) had investigated IIOC cases, with 37.2% having been involved in over 50 cases (37.2%).

4.2. Qualitative Analysis

This section elaborates on the themes which emerged from the analysis of practitioners' comments about challenges affecting the investigation of IIOC cases. These were grouped into two categories: generic challenges affecting IIOC cases, and IIOC-specific challenges, as summarised in Table 2.

Challenge Themes
Generic challenges (affect IIOC cases)
• Evolution of technology & offenders' skills
• Increasing volume of data to be investigated
• Lab management & commission of cases
• Limited resources available
• Evidence handling, analysis & reporting
• Insufficient cooperation
Specific challenges (typical to IIOC cases)
• Establishing nature/degree of the offence
• Difficulties of identification of victims
• Stressful working conditions
• Non-standardised operations & legal framework

Table 2: Overview of Challenge Themes.

Please note that this classification followed a bottom-up approach. Therefore, although the challenges listed under the IIOC-specific category may affect other types of case, comments collected from DF practitioners were focused on important issues particular to IIOC cases.

Generic challenges and IIOC-specific challenges are reviewed in Sections 5 and 6, respectively.

5. Generic Challenges Affecting IIOC Cases

This section discusses a group of challenge themes that are not specific to IIOC, but which aggravate the IIOC-specific challenges (Section 6).

5.1. Evolution of technology & offenders' skills

There were three specific challenges identified in relation to this theme.

The first was the evolution of technology increasingly acting as anti-forensics, i.e., preventing (or acting against) the availability or usefulness of evidence to the forensics process (adapted from [25]). Although these challenges have been identified by other researchers (e.g., [26, 27, 28]), they are particularly important in facilitating the storage, distribution and commercialisation of IIOC. Refer to Figure 1.

•*Storage of images and data being held in 'the cloud' is becoming more difficult to manage an offender having access even when devices are seized.*
•*Vendors offer free encryption of data, it takes more time to investigate the materials.*
•*Ineffectiveness in tracing criminal activity when data anonymization and obfuscation techniques have been employed.*
•*There are also challenges faced with encryption technologies and other anonymizers and privacy technologies TOR, true crypt, etc.*
•*Steganography/cryptography are the biggest challenges.*

Figure 1: Extract of comments related to the challenge theme "Evolution of technology & offenders' skills".

Another evolution mentioned by DF practitioners was the increasing level and sophistication of criminals' computing skills and knowledge, allowing them to take full advantage of such novel technology. These developments negatively impact investigators' ability to collect digital evidence destroyed or concealed by criminals and, therefore, to trace criminal activities and identify offenders and victims. They also increase time and effort spent on IIOC investigations. Refer to Figure 2.

•*Widespread availability of data sanitation and device wiping software for consumer devices which may lead to destruction of evidence.*
•*Offenders who have IT knowledge attempt hide their actions, which in turn makes it harder to prove a case.*
•*Trying to find first generation images when the meta data is striped from the image.*
•*Anti-Forensics actions.*
•*Offenders uses many security tools and systems to protect their data and cover any evidence!*

Figure 2: Extract of comments related to the challenge theme "Evolution of technology & offenders' skills".

Yet another facet of this challenge theme is the fast technological pace of changes and the unbalanced response in terms of adequacy of DF practices, tools and knowledge/skills of investigators. This reinforces the *urgency in closing gaps*, mentioned by Harichandran et al. [14]. Refer to Figure 3.

•*Electronic devices are changing all the time, the operating systems change so do the file structures. The software used needs to be constantly updated to obtain the data from the devices.*
•*. . . complexity of operating systems.*
•*Complexity of IT environment.*

Figure 3: Extract of comments related to the challenge theme "Evolution of technology & offenders' skills".

5.2. Increasing volume of data to be investigated

This challenge theme is broad and affects all types of DF investigation [29, 14]. However, factors like affordability of digital devices, increasing storage capacity in devices and memory cards, and inexpensive cloud storage simplify possession, production (promoted by high quality cameras embedded in portable devices) and sharing/distribution of IIOC. Tool support for efficient processing, review, and analysis (e.g., tagging, categorisation, carving) become vital not only for prosecution purposes, but also for safeguarding of victims. Refer to Figure 4.

•*Volume of exhibits and the size of data storage on each one.*
•*Excessive quantity of picture/video files to review and/or categorise.*
•*Many photos and videos to tag.*
•*Processing a case can take anywhere between two days to two months.*
•*Increasing amounts of storage space. Many investigations are multiple TB's of data.*
•*Inability to expediently locate relevant information amongst large sets of data.*
•*As storage increases in size I am finding processing (carving pictures and videos, etc) takes a very long time.*

Figure 4: Extract of comments related to the challenge theme "Increasing volume of data to be investigated".

Another aspect related to the volume of data to be investigated is the frequency of IIOC cases.

Practitioners mentioned that this increase in volume of cases to be investigated is not proportional to the resources allocated, therefore as other researchers have pointed out [14, 29, 30], the backlog of cases is increasing significantly for law enforcement. This is related to the next challenge theme of resource allocation. Refer to Figure 5.

- *. . . there is a huge amount if backlog of digital forensics cases building up at police stations. Thus more forensics personnel are required.*
- *The frequency of child pornography cases is increasing compared to the available resources to combat the situation.*

Figure 5: Extract of comments related to the challenge theme "Increasing volume of data to be investigated".

5.3. Lab management & commission of cases issues

DF practitioners highlighted how factors/decisions at the strategic level become challenges at the operational level. Comments also suggested that resource allocation may be influenced by cost (at the expense of the drive to safeguard all victims), personal preferences by managers regarding policies and political agendas. Refer to Figure 6.

- *Willingness of law enforcement agencies to commit resources to offending may depend on the extent to which an investigation or prosecution is congruent existing with policy preferences, public priorities, or political agendas.*
- *Police forces do not like higher invoices than the quoted for, so spending extra time on cases rarely happens, its all money related, sadly.*
- *The number of investigations per examiner.*

Figure 6: Extract of comments related to the challenge theme "Lab management & commission of cases".

Practitioners also highlighted the challenges associated with the nonexistence of an uniform framework guiding the commission of requests for IIOC investigations, as well as ineffective communication between attorneys and investigators. Such communication becomes difficult due to language barriers among computing and legal practitioners, probably derived from technical knowledge mismatch. However, DF investigators also pointed to the lack of willingness from legal commissioners to overcome such differences. Refer to Figure 7.

- *Lack of information or guidance from those requesting the work.*
- *Lack of technical knowledge of those requesting the work, and the lack of willingness to learn/hear about it.*
- *Language barrier between forensic examiners and attorneys/judges to explain why the existence of child porn does not prove guilt.*
- *Some attorneys may be unresponsive or may not provide us with all the discovery documentation containing the details related to the case so we may have to go in and pick apart the case from the ground up ourselves.*

Figure 7: Extract of comments related to the challenge theme "Lab management & commission of cases".

5.4. Limited resources available

The imbalance in resource availability for defense and prosecution was identified as one aspect of this challenge theme. They stressed that it may lead to miscarriages of justice. Refer to Figure 8.

- *. . . getting access to information. As a defense expert, sometimes it can be a pain to get approval by law enforcement to allow us to review for our client.*
- *Law enforcement has many tools at their disposal which are not available to non-law enforcement (defense) experts. This makes the justice system unequal, as we cannot fully defend clients.*

Figure 8: Extract of comments related to the challenge theme "Limited resources available".

Limitations on available resources for IIOC investigations was another facet raised. As revealed by practitioners, it covers the following aspects: funding, hardware, software (tools), time, and personnel. Both the public and the private sectors are subject to such constraints. Such shortages may impact, for example, examiners' ability to find all the evidence/safeguard victims, to identify exculpatory

evidence, and to utilise best practices in analysis. Refer to Figure 9.

- *Police who are not equipped with specialized tools for extracting information, or furnished with sufficient computational power to expediently process data, may miss critical evidence during analysis in the laboratory or while performing triage in the field.*
- *Being in the private sector... our time and resources are limited. Sometimes we don't have all the tools we need, or the time needed to conduct processes or a full timeline analysis.*
- *The quantity of data to be reviewed, if it were to be done properly, is too great for the time and funding available.*
- *Analysts and investigators who are unable to dedicate time towards identifying exculpatory sources of evidence may undermine the strength of a case or cause miscarriages of justice.*

Figure 9: Extract of comments related to the challenge theme "Limited resources available".

5.5. Evidence handling, analysis & reporting

This theme consisted of 4 specific challenges.

In terms of IIOC evidence handling, practitioners raised the non-compliance to best practices for sound acquisition/collection of evidence, ultimately resulting in evidence inadmissibility for the Court of Law – refer to Figure 10. This may relate to factors such as insufficient education/training [14], and over-reliance on "push-button forensics" [31].

In terms of evidence analysis, practitioners mentioned several deficiencies in tool support which had a strong link with the "volume" challenge theme (Section 5.2) related to performance. For example, they explicitly touched on the aspect of inadequacy of thumbnails for IIOC cases, issues with search for an image match, and also outdated hash sets for identification of known IIOC. Interestingly, over reliance on hash matching (based on archived images) was also mentioned. Refer to Figure 11.

As identified in Figure 12 – practitioners emphasised difficulty in decision making regarding *best evidence* in IIOC cases as a time consuming aspect of reporting to Court. They also mentioned the conscious effort required to maintain an unbiased and professional posture when stating conclusions, and reporting the facts of IIOC investigations to Court.

- *Lack of knowledge in gathering the actual evidence.*
- *Actually we get evidence collected by law enforcement or other customer mostly done without correct procedure, often it is contaminated.*
- *The work I do is primarily defence cases, so I'm supplied with electronic data by the prosecution (police), the problem we have on a regular occurrence is that officers do not understand the four principles of the ACPO guidelines for digital evidence.*

Figure 10: Extract of comments related to the challenge theme "Evidence handling, analysis & reporting issues".

- *Thumbnail pictures can be a pain, very little detail.*
- *Known hash sets are over relied upon.*
- *... out of date hash sets.*
- *Matching of Images when reference photograph provided.*

Figure 11: Extract of comments related to the challenge theme "Evidence handling, analysis & reporting".

- *Is this good evidence to send court?*
- *... extra effort required to resist the urge of getting prejudiced by what we see during the investigation (i.e. make a biased conclusion, or affect the way facts get stated and presented in the report in a way that might compromise the neutrality of the forensic process).*

Figure 12: Extract of comments related to the challenge theme "Evidence handling, analysis & reporting".

5.6. Insufficient cooperation

The theme of insufficient cooperation had a national and international scope.

At the national level, practitioners mentioned insufficient cooperation between prosecution (law enforcement) and defense (companies, consultants),

while at the international level they mentioned difficulties related to MLAT (Mutual Legal Assistance Treaties) and ILOR (International Letter of Request). The latter problem aligns with work by James and Gladyshev [32], who discussed specific challenges related to mutual legal assistance requests (MLAR). Uncooperative Internet Service Providers (ISP) was also highlighted as one facet of this challenge theme. Refer to Figure 13.

- *It was difficult to get access to the necessary information/data especially stored in foreign country.*
- *MLAT/ILOR*
- *Lack of cooperation from different organizations and abroad companies.*
- *Information sharing between prosecution and defence needs attention.*
- *. . . getting access to the information. As a defense expert, sometimes it can be a pain to get approval by law enforcement to allow us to review for our client.*
- *. . . the exact physical location, the ISP will not provide details and hide [of] information.*

Figure 13: Extract of comments related to the challenge theme "Insufficient cooperation".

6. Challenges Specific to IIOC Cases

6.1. Establishing nature/degree of the offence

One of the key themes which emerged from the analysis was the challenges associated with establishing the nature of the offence and identifying the offender.

Participants discussed difficulties in attributing ownership of devices or accounts on shared devices to an individual offender. This is an issue relevant to other categories of cybercrime, however, challenges associated with determining the nature of the offence/offending behaviour are unique to IIOC cases. This included whether the offender was involved in accessing and collecting images, and would therefore be charged with possession/making offences. It also required determining the presence of evidence of distribution of material, the associated methods by which this was achieved, and the related need to identify whether the individual was engaged in networking with other offenders, and the potential for offender's involvement in the production of images and associated sexual offences against children. Refer to Figure 14.

- *Where did it come from?*
- *How much material?*
- *Did the user spread material, if yes how much and to who?*
- *Difficulty in attributing ownership and authorship to electronically stored information.*
- *Difficulty in identifying individuals in control of information systems and devices. Find out if the offender is part of a network or not. if you have had accomplices.*
- *Trying to determine if the suspect is a trafficker or mere collector.*

Figure 14: Extract of comments related to the challenge theme "Establishing nature/degree of the offence".

6.2. Difficult identification of victims

The challenges associated with victim identification were also mentioned by some participants, and these formed three intertwined categories: establishment of victim identity, identification of victim age and identification of illegal content.

The first category referred to the difficulties for investigators in determining the identity of victims where this was unknown at the point of detection. This is common in cases where offender collections are recovered and analysed, and one of the aims of the investigation is to determine victims identity based on the information included in images/videos, as well as other related digital forensic evidence. This is also related to establishing whether the offender is involved in production of material and has access to the depicted victims in the offline environment [33] as described in relation to the previous themes (refer to Figure 15).

- *Trying to determine if there is an identifiable victim.*
- *To identify the real ID of the victims to discover if there are more victims.*

Figure 15: Extract of comments related to the challenge theme "Difficult identification of victims".

The second category related to the challenges of establishing the age of victims where their identity

was unknown. This can be difficult to determine when the victims appear to be older adolescents, and establishing their age is central to confirming whether an offence has occurred. It is also complicated by the potential for images to have been produced in the past, with the potential for the physical characteristics of victims to have changed, therefore, leading to the third category which was the identification of illegal content. Participants described the challenges associated with this aspect of investigations, and highlighted the need for clearer guidelines on how to achieve more effective categorisation. Again, some facets of this challenge theme may also apply to other crime categories, however, they are particularly relevant for IIOC cases. For example, identification of age is key in establishing the boundary between legal and illegal content. Refer to Figure 16.

•The general challenges that most investigators face are determination of the true age of victims in those case where the victim is not known and the images are not clearly of a child (pre-pubescent, infants, etc).
•Determine whether it is a child or not therefore all pornography will be added as evidence in a child porn case for the court to decide what is relevant.
•Determining the age of the victim. It is becoming increasingly difficult to ascertain whether someone is over or under the age of 18.

Figure 16: Extract of comments related to the challenge theme "Difficult identification of victims"

6.3. Stressful working conditions

Participants also highlighted the challenges associated with the emotional reactions and impacts of working with IIOC. Given the nature of the content of images and the victims depicted in them, prolonged exposure can have negative psychological impacts for those involved in evidence recovery and analysis, as well as investigators and legal practitioners. Refer to Figure 17.

6.4. Non-standardised operations/legal framework

Practitioners also highlighted legal and operational challenges related to the investigation of IIOC cases.

•Prolonged exposure to obscene material may create mental health issues for investigators, prosecutors, and forensic interrogators.
•Images of child abuse can be very disturbing and lead to negative impacts on the health of investigators.
•I find it difficult to look at child porn images. It has very adverse emotional effects. Staying unemotional in a case where a child had been abused to that extent is very cumbersome.

Figure 17: Extract of comments related to the challenge theme "Stressful working conditions".

Legal challenges were related to jurisdictional discrepancies in the boundaries between legal and illegal content in terms of IIOC. The lack of an internationally recognised classification of IIOC by level of severity also adds complexity to the issue. Refer to Figure 18.

•Getting fellow team members/investigators to agree as to what is considered CP based on the COPINE scale and findings ways to introduce COPINE scale within reports submitted. - Not recognised within UAE at present which means only more serious and obvious types of CP are considered/prosecuted.

Figure 18: Extract of comments related to the challenge theme "Non-standardised operations/legal framework".

Operational challenges pointed out by practitioners were mainly related to the sensitivity of IIOC evidence being highly regulated in some jurisdictions. The lack of uniform procedure, however, across public and private sectors, as well as across regional and national levels, raise discrepancies in authorisation and handling of IIOC cases. Refer to Figure 19.

7. Suggested Solutions to Theme Challenges

This section discusses suggested solutions to IIOC-specific challenges described by participants of the survey. Tables A1 and A2 of the Appendix contain additional suggestions for IIOC-

- *Due to the Child Protection Act, these examinations have to be done at a police facility, requiring the transportation of personnel and equipment.*
- *There is a need for regional and national standard operating procedures in relation to the discovery of indecent images by private sector investigations. These SOP's need to be created in partnership, but issued/endorsed by the private sector.*
- *(It's challenging) Obtaining Court Orders to handle/copy some of the material.*
- *In Scotland the police will not provide an imaged drive to investigate outside the police/PF facilities.*

Figure 19: Extract of comments related to the challenge theme "Non-standardised operations/legal framework".

specific challenges, and suggestions for generic challenges, respectively.

7.1. Nature/degree of offence

Participants made suggestions for improvements in this area which related to the importance of developing further understanding of offender motivations. They also mentioned the need for more detailed analysis of the available evidence to identify behavioural patterns which indicate the particular characteristics of the offender. Refer to Figure 20.

- *Trying to understand motivation is important.*
- *Behaviour patterns – does the suspect's computer use suggest that he/she is an avid pedophile?*

Figure 20: Extract of comments related to suggested solutions to the challenge theme "Establishing nature/degree of offence".

Suggestions by practitioners align with a body of literature which studies the applicability of Behavioural Evidence Analysis (BEA) to IIOC cases [34, 35]. Preliminary empirical evaluation (using DF evidence from actual IIOC cases) has indicated that BEA can in fact assist investigators in several aspects. For example, it helps to focus an investigation, enables better understanding and interpretation of victim and offender behaviour, and assists in inferring traits of the offender from available digital evidence [35]. However, caution should be taken to ensure objectivity in the use of this method, as expressed by the following comment by a practitioner who participated in the survey. Refer to Figure 21.

- *It is not part of my remit to speculate on the state of mind of the offender... As a Forensic Scientist I have to remain unbiased and simply show what exists without speculation.*

Figure 21: Extract of comments related to suggested solutions to the challenge theme "Establishing nature/degree of offence".

7.2. Identification of victims

Participants made suggestions related to the need for further research focusing on determining the age of victims, as well as the need for victim identification to be a more central focus for the work of investigators. Refer to Figure 22.

In the UK, e.g., the adoption of Streamline Forensic Reporting (SFR) [36] for IIOC cases [1] aims to deal with cases more efficiently and expeditiously by increasing the rate of early guilty pleas. This aims to reduce the number of cases which requires additional DF investigation [37]. The danger, however, is that prosecution (i.e., recovering sufficient evidence to allow prosecution) takes priority over victim safeguarding (i.e., recovering further evidence that may allow identification of all potential victims).

- *Age determination should become the subject of more research.*
- *More work towards possible victim identification and did the suspect participate in the manufacture of the illicit materials.*

Figure 22: Extract of comments related to suggested solutions to the challenge theme "Difficulties of identification of victims".

Automatic age estimation/classification using images is an active area of research [38, 39, 40]. However, it seems that this progress is not being translated into useful tools to assist the investigation of IIOC cases.

7.3. Working conditions

DF practitioners suggested better support for those dealing with IIOC investigations, and more R&D towards further automation leading to less exposure to IIOC imagery and recording. Refer to Figure 23.

A small number of studies have investigated the psychological and social impacts of exposure to such material in the course of the work of police officers and civilian staff [41, 42, 43, 44, 45]. These have identified a number of different psychological impacts, including negative emotional reactions (e.g. shock, distress, sadness, powerlessness, guilt), the experience of unwanted and intrusive thoughts and memories of images viewed, altered behaviour towards partners and children, and increased cynicism and suspiciousness of others [46, 42]. These studies highlight the need to ensure provision of effective supervision and support to staff working in these areas [42, 43, 47].

> •*Better support post-case for examiners.*
> •*Better/more reliable tools for minimizing exposure to content by examiners.*

Figure 23: Extract of comments related to suggested solutions to the challenge theme "Stressful working conditions".

There has been less focus on the potential impacts of exposure in digital forensic practitioners, though similar outcomes are to be expected, as indicated by the comments made by participants. This suggests that research and work in developing more effective support systems for staff should ensure the inclusion of this group of practitioners. It is also important that individuals engaged in this work and employed by private companies also receive sufficient support to respond to the challenges associated with exposure to this material as part of their job.

7.4. Standardisation of Operations/Legislation

Practitioners suggested standardisation of terminology in legislation and as way to improve effective communication between international law enforcement regarding IIOC investigations. They also suggested that international laws regarding IIOC should be enforced, and that a worldwide database of IIOC should be in place to facilitate the identification of offenders and victims. At the moment, there are national databases, such as the Child Abuse Image Database (CAID) in the UK, and Interpol's International Child Sexual Exploitation (ICSE) image database [48]. However, only member countries can access the ICSE which is problematic given the international nature of IIOC offending.

Yet another aspect would be the adoption of a standardised and internationally agreed scale for assessment of the indecency level of IIOC. Example scales are: the COPINE (Combating Paedophile Information Networks In Europe) scale with 10 levels, the SAP (Sentencing Advisory Panel) scale with 5 levels, and the simplified 3-levels scale (categories A-C), currently used in the UK [1].

Refer to Figure 24 for an overview of suggestions from DF practitioners.

> •*Definitions of offending must be expressed with precision, consistency, and formulated in consultation with the international community to be capable of overcoming language barriers and bridging cultural voids.*
> •*A worldwide database.*
> •*Standard international laws.*
> •*Getting fellow team members/investigators to agree as to what is considered CP based on the COPINE scale and findings ways to introduce COPINE scale...*

Figure 24: Extract of comments related to suggested solutions to the challenge theme "Non-standardised operations & legal framework".

8. Validity of Results

The sample size for the study was adequate, however, some caution must be exercised in terms of generalisability of the results. The majority of the respondents were male, but this is consistent with the gender composition of the workforce in this area. In fact, there is no specific reason to expect that males and females differ in terms of the identification of challenges and suggested solutions.

The dominance of European and North American participants also means that there may be some geographical region bias in the challenges and solutions identified. Despite this, the authors feel that the analysis of the issues highlighted by practitioners is sufficiently robust to identify a number of areas requiring further attention. This includes more

effective communication and practical implementation of research results, efforts to further improve legal cooperation at the national and international levels, and the need to develop effective support systems for the psychological well-being of practitioners investigating IIOC offending.

9. Conclusion

This paper reported on the results from a survey which collected text-rich comments from digital forensics practitioners active in IIOC investigations. Using Thematic Analysis, 10 challenge themes were identified and grouped into two categories.

Challenge themes specific to IIOC cases were: (1) complex establishment of nature/degree of the offence, (2) difficult identification of victims, (3) stressful working conditions for DF practitioners dealing with IIOC imagery/recording, and (4) non-standardised operations & legal framework. Although some of these challenges apply to other types of cases, comments received were elicited with specific focus on challenges associated with IIOC cases and were therefore grouped in this category. However, these issues are also relevant to the investigation of other categories of cybercrime. This highlights the need for further empirical and practical attention to be focused on addressing these issues in the broader context of DF investigations.

Generic challenge themes which aggravated those which were IIOC-specific were: (1) evolution of technology & offenders' (computing) skills, (2) increasing volume of data to be investigated, (3) lab management & commission of cases, (4) limited resources available, (5) evidence handling, analysis and reporting, and (6) insufficient cooperation. The identification of these themes are consistent with the results of previous research identifying generic challenges facing DF practitioners (e.g., [19, 14]). This indicates the need for a variety of actions to be taken by different stakeholders to develop appropriate challenges and related solutions.

The following key issues were identified by the analysis of the challenge themes and solutions suggested by practitioners:

1. Research advancements in areas, such as automatic estimation of age based on images/videos, are not being translated to workable tools to improve DF practice related to the investigation of IIOC.
2. Results also suggested that better understanding is required of the impacts caused by dealing with IIOC, related coping strategies, and automation to minimise exposure in the first place. This calls for more interdisciplinary research between Psychology, Computing, and Policing disciplines. It also requires a review of the current procedures used in digital forensics labs for supporting staff and early identification of those experiencing adverse effects as a result of exposure to IIOC.
3. Another interesting suggestion which emerged was the need for standardisation of operations and procedures, as well as of legal frameworks. This requires, among others, the adoption of an internationally recognised scale of indecency levels and a taxonomy of terms to bridge language and cultural differences.

Acknowledgements

We thank the Dubai Police General Head Quarters for sponsoring one author and unconditional support for this research.

References

[1] The Crown Prosecution Service, Indecent Images of Children, http://www.cps.gov.uk/legal/h_to_k/indecent_images_of_children/ (n.d.).

[2] The United States Department of Justice, Child Pornography, https://www.justice.gov/criminal-ceos/child-pornography (2017).

[3] CEOP, Threat Assessment of Child Sexual Exploitation and Abuse, https://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf [Accessed 15/08/17] (2013).

[4] NCA, National Strategic Assessment of Serious & Organised Crime, http://nationalcrimeagency.gov.uk/publications/731-national-strategic-assessment-of-serious-and-organised-crime-2016/file [Accessed 09/08/17] (2016).

[5] Global Alliance, Global Alliance Against Child Sexual Abuse Online – 2015 Threat Assessment Report, https://ec.europa.eu/home-affairs/what-is-new/news/news/2016/20160317_2_en (2016).

[6] NCA, National Strategic Assessment of Serious & Organised Crime, http://nationalcrimeagency.gov.uk/publications/731-national-strategic-assessment-of-serious-and-organised-crime-2016/file [Accessed 09/08/17] (2017).

[7] J. Pieters, Explosive Increase in Child Pornography Forms National Threat: Dutch Police, http://nltimes.nl/2017/05/31/explosive-increase-child-pornography-forms-national-threat-dutch-police [Accessed 10/08/17] (2017).

[8] T. Reith, Rise of social media leads to flood of child porn images, http://www.cbc.ca/news/canada/edmonton/social-media-exploitation-1.4130160 [Accessed 10/08/17] (2017).

[9] H. Bentley, O. O'Hagan, A. Brown, N. Vasco, C. Lynch, J. Peppiate, M. Webber, R. Ball, P. Miller, A. Byrne, M. Hafizi, F. Letendrie, How Safe Are Our Children?, https://www.nspcc.org.uk/globalassets/documents/research-reports/how-safe-children-2017-report.pdf [Accessed 09/08/17] (2017).

[10] A. Mojica, FBI issues sobering statistics on child pornography in the United States, dark web, http://fox17.com/news/local/fbi-issues-sobering-statistics-on-child-pornography-in-the-united-states-dark-web [Accessed 10/08/17] (2017).

[11] C. Johnston, Number of child sexual abuse claims overwhelming police, says lead officer, https://www.theguardian.com/society/2017/feb/28/child-sexual-abuse-claims-overwhelming-police-says-lead-officer [Accessed 10/08/17] (2017).

[12] M. Rogers, K. Scarborough, K. Frakes, C. S. Martin, Advances in Digital Forensics III, Springer, 2007, Ch. Survey of law enforcement perceptions regarding digital evidence, pp. 41–52.

[13] M. K. Rogers, K. Seigfried, The future of computer forensics: a needs analysis survey, Computers & Security 23 (2004) 12–1612–16.

[14] V. S. Harichandran, F. Freitinger, I. Baggili, A. Marrington, A Cyber Forensics Needs Analysis Survey: Revisiting the Domain's Needs a Decade Later, Computers & Security 57 (2016) 1–13.

[15] S. Liles, M. Rogers, M. Hoebich, Advances in Digital Forensics V, Springer, 2009, Ch. A survey of the legal issues facing digital forensic experts, pp. 267–276.

[16] H. Hibshi, T. Vidas, L. Cranor, Usability of forensics tools: a user study, in: Proceedings of the Sixth International Conference on IT Security Incident Management and IT Forensics (IMF), IEEE, 2011, pp. 81–91.

[17] K. Ruan, J. Carthy, T. Kechadi, I. Baggili, Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results, Digital Investigation 10 (1) (2013) 34–43.

[18] M. Al Fahdi, N. L. Clarke, S. M. Furnell, Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions, in: Proceedings of the 2013 Information Security for South Africa Conference (ISSA), IEEE, 2013, pp. 1–8.

[19] P. Amann, J. I. James, Designing robustness and resilience in digital investigation laboratories, Digital Investigation 12 (2015) S111–S120.

[20] J. R. Draugalis, S. J. Coons, C. M. Plaza, Best practices for survey research reports: a synopsis for authors and reviewers, American journal of pharmaceutical education 72 (1) (2008) 1–6.

[21] B. A. Kitchenham, S. L. Pfleeger, Principles of survey research – Part 3: Constructing a survey instrument, ACM SIGSOFT Software Engineering Notes 27 (2) (2002) 20–24.

[22] V. Braun, V. Clarke, Using Thematic Analysis in Psychology, Qualitative Research in Psychology 3 (2) (2006) 77–101.

[23] J. Bryce, J. Fraser, The role of disclosure of personal information in the evaluation of risk and trust in young peoples online interactions, Computers in Human Behavior 30 (2014) 299–306.

[24] C. Robson, Real world research: A resource for users of social research methods in applied settings, 3rd Edition, West Sussex: John Wiley & Sons, 2011.

[25] Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, Digital Investigation 3 (2006) S44–S49.

[26] E. Casey, G. Fellows, M. Geiger, G. Stellatos, The growing impact of full disk encryption on digital forensics, Digital Investigation 8 (2) (2011) 129–134.

[27] S. Raghavan, Digital forensic research: current state of the art, CSI Transactions on ICT 1 (1) (2013) 91–114.

[28] A. Phelps, A. Watt, I shop online recreationally! Internet anonymity and Silk Road enabling drug use in Australia, Digital Investigation 11 (4) (2014) 261–272.

[29] D. Quick, K.-K. R. Choo, Impacts of increasing volume of digital forensic data: A survey and future research challenges, Digital Investigation 11 (4) (2014) 273–294.

[30] D. Lillis, B. Becker, T. O'Sullivan, M. Scanlon, Current Challenges and Future Research Areas for Digital Forensic Investigation, http://arxiv.org/abs/1604.03850 [Accessed 12/08/17] (2016).

[31] J. James, P. Gladyshev, Challenges with Automation in Digital Forensic Investigations, https://arxiv.org/abs/1303.4498 [Accessed 12/08/17] (2013).

[32] J. I. James, P. Gladyshev, A survey of mutual legal assistance involving digital evidence, Digital Investigation 18 (2016) 23–32.

[33] M. Long, L. Alison, R. Tejeiro, E. Hendricks, S. Giles, KIRAT: Law enforcements prioritization tool for investigating indecent image offenders, Psychology, Public Policy, and Law 22 (1) (2016) 12–21.

[34] M. K. Rogers, K. C. Seigfried-Spellar, Using Internet Artifacts to Profile a Child Pornography Suspect, Journal of Digital Forensics, Security and Law 9 (1) (2014) 57–66.

[35] N. A. Mutawa, J. Bryce, V. N. L. Franqueira, A. Marrington, Behavioural Evidence Analysis Applied to Digital Forensics: An Empirical Analysis of Child Pornography Cases uing P2P Networks, in: Proceedings of the 10th International Conference on Availability, Reliability and Security (ARES), IEEE, 2015, pp. 293–302.

[36] The Crown Prosecution Service, Streamlined Forensic Reporting Guidance and Toolkit, http://www.cps.gov.uk/legal/s_to_u/scientific_evidence/sfr_guidance_and_toolkit/ [Accessed 24/09/17] (n.d.).

[37] The Crown Prosecution Service, National Streamlined Forensic Reporting Guidance, http://www.cps.gov.uk/legal/assets/uploads/files/toolkit_sfr_section_1_2015_cpr_revision_final.doc(LastUpdated20December2016) [Accessed 24/09/17] (2015).

[38] A. Lanitis, C. Draganova, C. Christodoulou, Comparing Different Classifiers for Automatic Age Estimation, Transactions on Systems, Man, and Cybernetics 34 (1) (2004) 621–628.

[39] K. Luu, K. R. Jr., T. D. Bui, C. Y. Suen, Age Estimation using Active Appearance Models and Support Vector Machine Regression, in: Proceedings of the 3rd Int. Conf. on Biometrics: Theory, Applications, and Systems (BTAS'09), IEEE, 2009, pp. 1–5.

[40] S. E. Choi, Y. J. Lee, S. J. Lee, K. R. Park, J. Kim, Age estimation using a hierarchical classifier based on global

and local facial features, Pattern Recognition 44 (6) (2011) 1262–1281.

[41] S. W. Craun, M. L. Bourke, The use of humor to cope with secondary traumatic stress, Journal of child sexual abuse 23 (7) (2014) 840–852.

[42] S. W. Craun, M. L. Bourke, F. N. Coulson, The Impact of Internet Crimes against Children Work on Relationships with Families and Friends: An Exploratory Study, Journal of Family Violence 30 (3) (2015) 393–402.

[43] R. Parkes, N. Graham-Kevan, J. Bryce, You don't see the world through the same eyes anymore: The impact of sexual offending work on Police staff, under review.

[44] M. Powell, P. Cassematis, M. Benson, S. Smallbone, R. Wortley, Police officers strategies for coping with the stress of investigating Internet child exploitation, Traumatology: An International Journal 20 (1) (2014) 32.

[45] M. Krause, Identifying and managing stress in child pornography and child exploitation investigators, Journal of Police and Criminal Psychology 24 (1) (2009) 22–29.

[46] C. M. Burns, J. Morley, R. Bradshaw, J. Domene, The emotional impact on and coping strategies employed by police teams investigating internet child exploitation, Traumatology 14 (2) (2008) 20–31.

[47] M. Powell, P. Cassematis, M. Benson, S. Smallbone, R. Wortley, Police officers perceptions of their reactions to viewing internet child exploitation material, Journal of Police and Criminal Psychology 30 (2) (2015) 103–111.

[48] Interpol, Databases – Fact Sheet, https://www.interpol.int/en/News-and-media/Publications2/Fact-sheets/Databases/ [Accessed 14/08/17] (2017).

Nature/degree of offence	I have used COPS (Child Online Protective Service) system from INTERPOL. It was very useful to investigate child porn distributors.
	. . . create a hash set of adult porn to use as a negative hash set to eliminate a significant amount of pictures and videos an examiner has to review today.
	Pictures (when possible) should be put into context (i.e. which website they come from).
	Pivotal to the success of investigations and prosecutions involving child pornography is the development of in-house subject matter experts to run complex cases and direct technical inquiries.
	. . . build a special group of many different skills.
	Google should also allow for searching of information related to child pornography.
Identification of victims	Greater resources for more thorough investigations and potential victim identification.
	More and easier sharing of hash sets of child pornography images.
	A trade-off is required as to whether being thorough in one case is more vital that investigating numerous cases.
	Ability to train investigators to obtain more information from the first encounter of the suspect. Better searches for passwords while at their residence.
	I recently uncovered a child porn picture which was too small to make out from the thumbnail, so I left the thumbnail small and photographed it with a high resolution camera, then enlarged the photo instead of the thumbnail. . . The imagery was much clearer and the case was extended.
	Up-to-date hash lists.
	More cooperation with physiological doctors
	Use of streamlined Forensic reports getting an early guilty plea.
Working conditions	Simplify categorization process.
	Smarter review of child abuse material (saves time) and data analysis (already some experience with it).
	More powerful porn detection modules.
	Better/more reliable tools for minimize exposure to content by examiners.
	Better support post-case for examiners.
Towards standardisation	A uniform taxonomy for criminal justice systems and legislative bodies is indispensable for achieving greater harmony among national and international legal frameworks.
	Better use of digital and real world intelligence.
	There is a need to introduce uniform and thorough cybercrime reporting mechanisms for addressing child pornography, globally.
	Clear guidelines on classification.
	Licensed investigators registered with the local law enforcement authority to undertake investigations involving this material. Central register of licensed investigators.
	Central information reference point available to non-law enforcement, e.g. hash sets of know child pornography.

Table A1: Further suggestions collected from practitioners for IIOC-specific challenge themes.

Volume of data	Legislative time constraints pertaining to the examination of data on information systems must adapt and evolve given exponential increases in consumer storage capacity and the complexity of extracting records from devices. This must be done to ensure that large quantities of data seized by police are sufficiently analyzed.
Lab management	To build multidisciplinary teams, law enforcement agencies require increased training and procurement budgets and clear opportunities for career progression to encourage recruitment and retention of talent.
	Digital forensic examination and CP crime investigation are in different tracks of cybercrime. They should be assessed separately.
	More training.
Resources	Increase in man power and budgets.
	Large servers to process evidence quickly.
	More staff to complete the work faster.
	Updated digital forensic tools.
	Very good triage techniques.
Evidence	To best assist fact-finders, courtrooms must be equipped with multimedia technology so that witnesses can effectively present results and convey meaning to essential aspects of the evidence.
	For the investigators to conduct a forensically secure PREVIEW of the data prior to requesting a full forensic exam. This should reduce the forensic lab's back log and allow the investigators to pursue there investigation more rapidly.
	Having an option to be able access 'cloud' storage to gain further evidence.
	Properly see all the files with headers not by the extensions.
	More tools need to be developed to support these types of investigations and to help identify and build timelines with auto-artifact inclusion.
	Forensic analysis tools that enable to analysts and researchers to label videos and photos in the same time and in the same case.
Cooperation	Bring countries on board that do not participate in child pornography watch lists.
	I suggest greater collaboration on the part of law enforcement agencies around the world to identify children present in [photo] shooting.
	Make tools available to all parties involved - law enforcement and defense.
	Simplification of procedures for obtaining the log files from network operators, service providers, etc.
	Child porn evidence should be examined as big data and information about images and videos should be exchanged between jurisdictions.

Table A2: Suggestions collected from practitioners for generic challenge themes.