Forensic Science International: Digital Investigation 51 (2024) 301839

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

“What you say in the lab, stays in the lab”: A reflexive thematic analysis of current challenges and future directions of digital forensic investigations in the UK

Magdalene Ng[a,*], Jade James[a], Ray Bull[b]

[a] University of Westminster, UK
[b] University of Derby, UK

ARTICLE INFO

Keywords:
Digital forensics
Police
AI
Automation
Court
Digital investigations
Digital evidence

ABSTRACT

Despite digital evidence nowadays playing a major role in criminal investigations and being intrinsic to almost every criminal trial, research in digital forensics (DF) and national approaches to digital evidence in relation to investigating officers and court personnel remain almost non-existent. This research seeks to remedy this issue by qualitatively examining the accounts and experiences of 16 digital forensic investigators (DFIs) in England and Wales who took part in semi-structured interviews. We analyzed the data using a reflexive thematic analysis and identified four overarching themes: (i) Navigating tensions with investigating officers (that has a subtheme of ‘Tensions with legal professionals and challenges navigating court theatrics’) (ii) The psychological, emotional, and existential challenges confronted by DFIs; (iii) Identifying the potential and pitfalls of automation and AI in DF and (iv) The centrality of academia in the advancement of DF (that has a subtheme of ‘Validation of tools as a crucial step in digital forensics’). These new findings reveal that DFIs encounter significant demands to perform well and are continuously overburdened while juggling many roles. This research serves as a pivotal starting point for broader discussions.

1. Background

1.1. Introduction to digital forensics

Digital forensics (DF) emerged in the 1980’s, making it a relatively young discipline (Pollitt, 2010) that evolved from forensic science (Kessler and Carlton, 2020; Page et al., 2019). Digital information found on digital devices such as personal computers can be relevant in the investigation of a wide variety of crimes (Lawton et al., 2014)—this is known as digital evidence. Locations where digital evidence can be stored include computers, laptops, hard drives, tablets, mobile devices, cloud storage, emails, network servers, IoT devices, and social media platforms (College of Policing, 2024; Miller, 2023).

Digital evidence shares some similarities with physical evidence, in that both help establish causality in criminal cases by connecting individuals and events to specific times and places. However, digital evidence differs from physical evidence in several important ways (Goodison et al., 2015; Kessler and Carlton, 2020). For instance, digital evidence is more volatile in that it is more susceptible to being compromised and destroyed compared to physical evidence. Additionally, crimes involving digital evidence can span multiple jurisdictions (Horsman, 2017). Crucially, DF is evolving at a rapid pace compared to traditional forensics due to growth of technology and the Internet, including the rise in child pornography cases and significant events like 9/11 (Johnson and Riemen, 2019; Pollitt, 2010).

Digital evidence is encountered in various crimes including murder, traffic accidents, intellectual property crimes (Piper, 2023), fraud, assault, arson (Goodison et al., 2015), sexual offenses (Belshaw and Nodeland, 2022), as well as terrorism and national security (McEwen, 2021). An early example of how digital evidence can be crucial in solving complex crimes is the case of Dennis Rader. Rader was an American serial killer who called himself the ‘BTK’ because he bound, tortured, and killed his victims (The Independent, 2023). Rader was captured in 2005, a time when DF was still in its infancy. Investigators traced him through metadata on a floppy disk that he had sent to the police (Sammons, 2014).

[*] Corresponding author. Magdalene Ng, 6.118, 115 New Cavendish St., University of Westminster, London, W1W 6UW, UK.
E-mail address: m.ng1@westminster.ac.uk (M. Ng).

https://doi.org/10.1016/j.fsidi.2024.301839
Received 16 November 2023; Received in revised form 24 September 2024; Accepted 1 October 2024

1.2. From crime scene to courtroom

Digital forensic investigators (DFIs) play a vital role in investigating crimes and other illegal activities conducted through digital platforms. They are experts who specialize in the acquisition and extraction of data from a variety of digital devices in a forensically sound manner, using specialized tools and technical skillsets (Morris et al., 2023). They are also competent in analyzing and preserving digital evidence. DFIs may opt to specialize in specific areas such as computers or mobile phones (Morris et al., 2023). The remit of their roles and responsibilities can vary across organizations, but in England, guidelines such as the Forensic Science Regulator: Codes of Practice and Conduct, British Standards IS017025 and the International Laboratory Accreditation Cooperation (ILAC) – G19: Modules in a Forensic Science Process, provide guidance as to what is expected of a DFI (Home Office, 2021; ILAC, 2022). DFIs are required to complete regular training courses to keep up-to-date with the latest tools and technology. Digital forensics certifications from industry vendors such as Magnet Forensics, Cellebrite, and MSAB are also essential requirements with most DFI roles (Cellebrite, n.d.; Magnet Forensics, 2023; MSAB, n.d.).

Digital investigations typically follow these six steps: 1) collection, 2) identification, 3) extraction, 4) analysis, 5) documentation, and 6) presentation (Casey and Schatz, 2011; Interpol, 2023)—as illustrated in Fig. 1. In the identification phase, DFIs define the scope of the investigation, determining which types of digital evidence are relevant to the case. DFIs may also request additional sources of digital evidence from the officer in charge (OIC) during this phase, and this process can be iterative. In the extraction phase, DFIs make sure digital data is carefully extracted from devices. In the analysis phase they reconstruct events from these data to determine what occurred and who was involved (Montasari, 2017) which has significant implications in criminal investigations, playing a crucial role in establishing culpability. Unlike traditional forensics, information extracted from digital devices is not directly comparable to a pre-established database of actions (Kessler and Carlton, 2020). Instead, DFIs work by generating hypotheses, investigating them, and confirm or deny their hypotheses about what has occurred and who was present. This leads to a unique investigative approach in this field. In the documentation phase, all findings are documented and reports are prepared in a format that is accessible to non-experts. In the presentation phase, DFIs may serve as a professional or expert witness in court or other legal settings, where they explain the digital evidence they uncovered and conclusions drawn from the evidence.

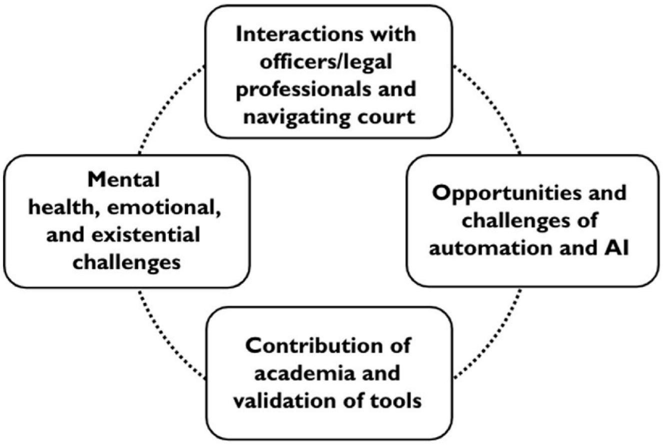
Interactions with officers/legal professionals and navigating court
Opportunities and challenges of automation and AI
Contribution of academia and validation of tools
Mental health, emotional, and existential challenges

Fig. 2. Thematic map of current keys challenges and perspectives of DFIs.

DFIs are often not present at crime scenes themselves to collect digital evidence (Wilson-Kovacs, 2021); a national shortage of digital media investigators (DMIs) means that police officers often conduct searches involving digital evidence. The few available studies on DF in relation to the police service have identified that law enforcement officers are facing challenges that affect their abilities to effectively respond to searches and seizures involving digital evidence. Given the enormous challenges of their role, police officers often struggle to meet the scale of digital crime, are understaffed, and undertrained (Barber Sir, 2020; Belshaw, 2019; Belshaw and Nodeland, 2022; Hadlington et al., 2021; Harichandran et al., 2016; Holt et al., 2020; Schreuders et al., 2018; Thompson and Manning, 2021; Wilson-Kovacs, 2021). While the perception of police officers investigating cybercrimes (a field related to DF) has received some attention (Hadlington et al., 2021), there is currently no research examining the experiences of DFIs and their interactions with police officers. Similarly, the DFIs' interaction with legal professionals is under-researched despite their significant responsibility in court outcomes. Existing studies, mostly conducted in the United States, have found limited technical understanding among judges and skepticism towards digital evidence (Cosic, 2017; Cummins Flory, 2016; Endicott-Popovsky and Horowitz, 2012; Kessler, 2010; Miller, 2023; Piper, 2023; Sommer, 2011). No studies have directly examined the

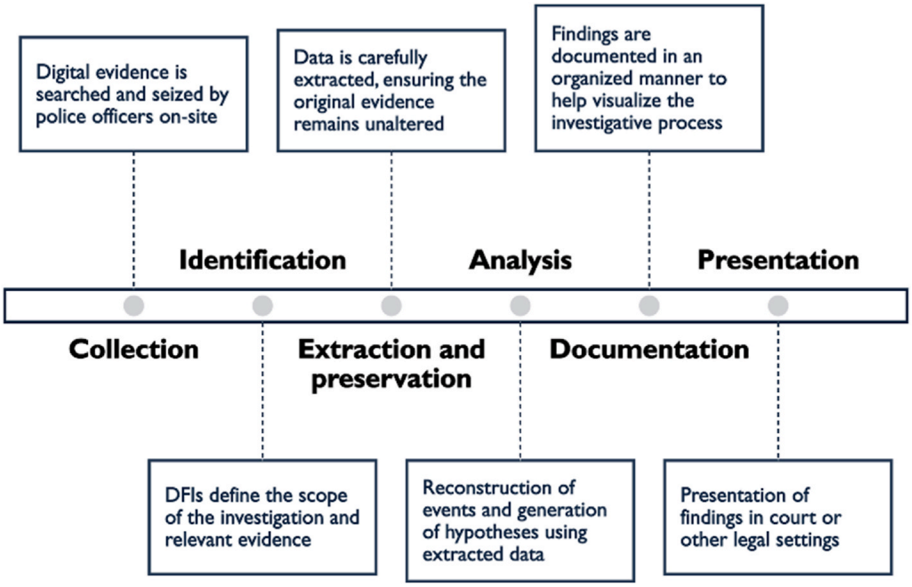
Digital evidence is searched and seized by police officers on-site
Data is carefully extracted, ensuring the original evidence remains unaltered
Findings are documented in an organized manner to help visualize the investigative process
Identification
Analysis
Presentation
Collection
Extraction and preservation
Documentation
DFIs define the scope of the investigation and relevant evidence
Reconstruction of events and generation of hypotheses using extracted data
Presentation of findings in court or other legal settings

Fig. 1. The six steps of a typical digital investigation.

experiences of DFIs, particularly in the context of their interactions with police officers and legal professionals—highlighting a critical research gap.

1.3. Challenges and developments in digital forensics

Digital evidence is now central to criminal investigations, present in over 90 % of cases in England (NPCC, 2020). This high percentage reflects a shift in digital evolution, resulting in an overwhelming volume of digital evidence for DFIs to extract and analyze (Goodison et al., 2015; Kelly et al., 2020; Sokol et al., 2020; Vincze, 2016). The proliferation of digital devices and rapid technological advancements have introduced new challenges in DF, such as the growing need for automation in forensic tools and tools with the ability to extract data from an increasingly diverse array of devices. The integration of automation and AI to support digital forensics has been gaining traction, despite being in its very early stages of development (Dunsin et al., 2023; James and Gladyshev, 2013). Scholars acknowledge that its incorporation in DF can simplify many of its processes (Dunsin et al., 2023), reduce investigator stress, and bolster accuracy, such as in cases of age estimation in indecent images (Grübl and Lallie, 2022; Jarrett and Choo, 2021). UK government initiatives, including the Police Digital program, aim to advance DF tools which are in their early stages of development (Police Digital Service [PDS], 2022).

In response to the growing volume of digital evidence, dedicated units have been established to address these demands such as the Regional Organised Crime Units (ROCUs) in the UK (Regional Organised Crime Units, n.d.). Additional challenges include the lack of rigorous quality control standards found in traditional forensics (Kessler and Carlton, 2020; Page et al., 2019), as DF is still a relatively new discipline. Indeed, in its current state, DF lacks established industry best practices for evaluating digital evidence, and many of its practices still need substantiation. To address quality assurance, the Forensic Science Regulator introduced the ISO/IEC 17025 for digital forensic providers in England and Wales. This standard ensures impartiality, validity, traceability, and objectivity in the forensic process (Marshall, 2010; Tully et al., 2020). Service providers are required to validate and verify their methods and tools, ensuring that evidence can withstand scrutiny in court in terms of evidence credibility, reliability, and integrity (Marshall, 2010; Slay et al., 2009). Despite criticisms of being outdated (Horsman, 2020), the Association of Chief Police Officers (ACPO)'s Good Practice Guides for Digital Evidence is still followed by DFIs in England and Wales (Kessler and Carlton, 2020). The Forensic Science Regulator requires digital forensic service providers to be competent several key processes of DF, including capture and preservation from digital media, screening or recovery of data from a device using an off the shelf tool (OST) for factual reporting, network capture and/or analysis, cell site analysis and communications data, and Internet intelligence and investigation including open-source intelligence (OSINT) from the internet. In order for digital forensics service providers to conduct digital forensics investigations and analyses, they must follow the guidance outlined in ISO/IEC 17020 or ISO/IEC 17025 and be accredited by UKAS, for the appropriate process (UKAS, n.d.). Therefore, if a laboratory is only accredited by UKAS to capture and preserve data from digital media, any other digital forensics processes applied to the digital data may result in a miscarriage in justice, as the digital data or evidence may become in admissible in a court of law. Proficiency testing and inter-laboratory comparisons are also key to ensure the quality of evidence produced and submitted into the criminal justice system will be upheld under scrutiny. Laboratories will routinely participate in exercises provided by external providers, to ensure that their methods and processes are compliant with the required standards.

1.4. The present study

Given that DF is dynamic and rapidly evolving, with unique challenges as summarized in Table 1, the current research aims to (i) identify key challenges DFIs in the UK face, (ii) gain insights into their interactions with investigative officers and court personnel, (iii) gather their views on ISO/IEC 17025 accreditation, (iv) explore perceptions of AI and automation in DF, and (v) evaluate the potential contribution of academia to the field.

2. Methodology

2.1. Participants

16 experienced DFIs from police forces across England and Wales were recruited through snowball and expert sampling that involved reaching out to investigators via personal contacts, LinkedIn, and social media posts endorsed by organizations like Forensic Focus and NPCC Forensic Capability Network. All participants have extensive expertise in DF and were interviewed individually online. The majority of the investigators identified as male ($n = 13$), with 3 identifying as female. Participants' level of relevant experience ranged from 2 years to 9 months to 16 years and 3 months, and the average is 8 years and 7 months.

2.2. Materials

Participants engaged in one-on-one interviews guided by a schedule (see Appendix A) developed through collaboration and discussions among all of the current authors (see Appendix B). The questions covered any investigative challenges encountered in their line of work, how they interact with different stakeholders during the investigative process, and their perspectives on national standards and requirements. Lastly, they were asked about their views on aftercare provided by their organizations and also to provide any final thoughts.

2.3. Procedure

The participants were provided with informed consent forms before interviews that mentioned the ensuring of confidentiality and

Table 1
Current landscape of Digital Forensics in the UK.

Aspect	Summary Overview
Evolution	Emerged in the 1980s, driven by technological advances.
Digital evidence	Digital evidence plays a critical role in various crimes (e.g., terrorism, sexual offenses).
Current state of digital evidence	Present in over 90% of criminal cases; large volumes of data from devices create challenges; AI and automation are being used to assist. Programs like *Police Digital* aim to improve DF tools and processes, focusing on AI and automation to ease DFI workload and improve accuracy.
Current list of studies and surveys of police officers, court personnel, DFIs, and DMIs	Belshaw (2019); Belshaw and Nodeland (2022); Barber Sir, 2020; Cosic (2017); Cummins (2016); Endicott-Popovsky and Horowitz (2012); Goodison et al. (2015); Hadlington et al. (2021); Harichandran et al. (2016); Holt et al. (2020); Kessler (2010); Miller (2023); Piper (2023); Schreuders et al. (2018); Sommer (2011); Thompson and Manning (2021); Wilson-Kovacs (2021).
Quality control and guidelines in the UK	ISO/IEC 17025; ISO/IEC 17020; ACPO Good Practice Guides; Forensic Science Regulator: Codes of Practice and Conduct; International Laboratory Accreditation Cooperation (ILAC) – G19: Modules in a Forensic Science Process.

anonymity. Interviews, conducted via MS Teams by the current first and second authors (MN and JJ), were audio-recorded and transcribed, with identifying information removed. Interview duration averaged 1 hour and 38 minutes (ranging from 52 minutes to 2 hours and 9 minutes). Afterwards, participants received debriefs with contact details of the research team should they have further questions about the study. They were issued a £15 gift voucher in recognition of their time given to the study.

2.4. Reflexive thematic analysis

After transcribing the interviews, pseudonyms were assigned to them to ensure participant anonymity. We then conducted a reflexive thematic analysis, following the six stages by Braun and Clarke (2019; 2021)—outlined in Table 3.

This iterative approach involved multiple rounds of coding and reviewing which allowed for a deeper understanding of the data, with expert guidance from Dr. Tina Cartwright. A reflexive statement is provided (Appendix B) reflecting on all authors' influences on the research process.

3. Findings

We identified four themes and two subthemes: (i) Navigating tensions with investigating officers; Subtheme: Tensions with legal professionals and challenges navigating court theatrics; (ii) The psychological, emotional, and existential challenges confronted by DFIs; (iii) Identifying the potential and pitfalls of automation and AI in digital forensics, and (iv) The centrality of academia in the advancement of digital forensics; Subtheme: Validation of tools as a crucial step in digital forensics. The themes are illustrated in a thematic map in Fig. 2. This figure illustrates how an increase in digital evidence and crimes involving digital evidence relates to our main findings; such as police officers and court personnel facing difficulties with digital evidence, as well as mental health, emotional, and existential challenges in DFIs.

Table 2 illustrates the array of criminal offenses and digital devices our participants encounter in their line of work, the majority of their caseload involving indecent images, sexual abuse, and grooming. We note that they are increasingly encountering cases involving vehicles, cloud forensics, IoTs, and drones, as also noted by Montasari and Hill (2019).

Table 2
Range of criminal offenses and digital devices encountered by DFIs in our sample.

Types of Criminal Offense	Types of Digital Device
Indecent images	Mobile devices (e.g., mobile phones, iPads)
Murder	Laptops/Computers/Chromebooks
Missing persons	CCTVs
Rape	USBs
Stalking	Drones
Domestic abuse	Internet of Things (IoTs) (e.g., voice-activated assistants, smart refrigerators, thermostats, doorbells, wearable technologies, fitness trackers)
Arson	Smart devices (e.g., TVs, watches, doorbells, drones, payment cards, water meters)
Sexual abuse	Internet of Vehicles (IoVs) (e.g., Teslas, BMWs)
Theft (i.e., intellectual property)	Cloud (e.g., TikTok, Snapchat, WhatsApp, other messaging applications)
Shoplifting	
Counterterrorism	
Radicalization	
Assaults	
Distribution of Class A, Class B drugs	
Distribution of firearms	
Grooming	
Kidnapping	
Human trafficking	
Defamation lawsuits	
Cryptocurrency and Bitcoin scams	
Payment card forensics	

Table 3
Six stages of Reflexive Thematic Analysis applied to DFI Interview Data.

Phase	Description of the Process
1. Familiarization	MN and JJ first familiarized themselves with the interview data, taking initial notes.
2. Generating Codes	Coding, which involves systematically labeling relevant sections of the transcripts, was approached both deductively (using predefined codes) and inductively (remaining open to new codes beyond the original framework).
3. Combining Codes into Themes	Once codes were generated, related codes were grouped into potential themes to capture broader patterns.
4. Reviewing Themes	Themes were reviewed and refined in this stage, and a thematic map was generated (see Fig. 2).
5. Defining and Naming Themes	Themes were clearly defined and named in this stage to reflect their core meanings.
6. Producing the Report	Final analysis of selected extracts (relating back to the research questions) were produced, as presented in Section 3: Findings.

3.1. Theme one: navigating tensions with investigating officers

Considering the diverse responsibilities of police officers and the relatively young field of DF, participants expressed concern over police officers' limited understanding of digital evidence, affecting what they seize, the quality of evidence seized, and their handling of the evidence. Our findings reveal that the proliferation of technological devices, coupled with their constant evolution, further creates challenges for police officers entering a scene that involves digital evidence. This finding highlights concerns not fully addressed in prior studies. Participants in our sample expressed that police officers "let the phones ring afterwards just to take numbers down" (Participant CL) and "have a quick look through the phone" (Participant NX). Other relevant comments include:

> "I've done warrants in my current role where police officers saying to me "What is this? Do I seize it, do I not?.. I've just come across what we think is a server and we go, 'No, no, no that's a television remote. You don't need to seize that'." (IX)

Participants expressed a lack of awareness amongst police officers regarding the multiple ways digital evidence can be retrieved (such as not needing the victim's phone, as victims can just send the data via a link to submit files or documents, or alternatively, the victim can be requested to attend a station). Participant IX mentions that "trying to get people to understand that there are four different ways of getting digital data" is a struggle. Officers also lack understanding of cloud systems and IoTs, sometimes missing critical evidence like a ring doorbell in an arson case (Participant NE).

> "Cloud data … it's such a big shift in police officer mindsets to understand that the device that has just been seized might not have the data that I want on it. It's like great, I've seized this phone, I've seized this laptop, you know, tea and medals, go home, suspects locked up. Not understanding that once we release them, they can log on from somewhere else and delete it all." (IX)

Participants revealed that police officers often lack awareness of issues such as data encryption and the Regulation of Investigatory Powers Act (2000) Section 49 (RIPA, 2003) ("We get still get on submission forms, you know, 'suspect not asked'" (PO)).] Section 49 provides power to serve a person of interest a RIPA notice, where this requires them to disclose passcodes and passwords (RIPA, 2003).]

3.2. Subtheme: tensions with legal professionals and challenges navigating court theatrics

Participants echoed frustrations with the broader legal system (Participant NX mentioning "we always used to refer it to it not as the Crown Prosecution Service, but as Couldn't Prosecute Satan"). This issue is further compounded by a perceived lack of preparedness exhibited by court personnel as well as their general lack of familiarity with technical terminologies, where Participant HY refers to the fundamental problem of them "not understanding what the data means". Participants commented that lawyers often misinterpret and confuse terminologies, leading to difficulties when DFIs write reports and present evidence to juries. This reflects a challenge in conveying evidence to the Crown Prosecution Service. Equally, participants highlighted significant challenges faced in translating evidence to the jury well, indicating a current deficit in their skills. They demonstrated awareness that as expert or professional witnesses they play a crucial role, as they can substantially influence the jury. Participants felt unprepared for court, needing better training beyond the currently available courses (e.g., Solon, 2019).

Participants mentioned being daunted by navigating court theatrics, referring to "the theatrics of court and everything that goes with it … you've got to kind of play the game of … lawyers back and forth" (Participant DM) and "Do your best not to break down and cry" (Participant IX). They also preferred not to be referred to as an 'expert witness' in court, as this puts pressure and creates confusion over their role. The difference between being a 'professional witness' and an 'expert witness' carries legal weight (Piper, 2023), and this is particularly salient in DF. In traditional forensics, there are definitive results, like fingerprints and DNA. However, DF results are open to interpretation, restricting DFIs to providing opinions on the available data and its conditions (Kessler, 2010; Sunde and Dror, 2019). Typically, witnesses provide unbiased accounts, but prosecutors and defense lawyers often ask DFIs for opinions based on their expertise, leaving participants grappling with their role in court and the high-stakes nature of courtrooms. This aspect introduces current findings that have not been covered in prior studies.

Participants suggested that fostering professional rapport with police officers and legal professionals can alleviate such tensions and enhance the quality of digital evidence seized and court proceedings. Elaborating on strategies to build rapport, participants revealed that this requires investment and time. Participant RH proposes that this process is dyadic and can be cultivated through repetition and open communication. Evidently, the challenges DFIs face in liaising with police and judicial staff are multi-faceted, deserving more consideration in future.

3.3. Theme two: the psychological, emotional, and existential challenges confronted by DFIs

Participants shared accounts of trauma due to frequent exposure to highly distressing scenes and materials, with most cases involving indecent images. This aligns with Tehrani's (2023) research, which found forensic investigators experience higher levels of anxiety, depression, and PTSD compared to other police staff. The current participants described pervasive feelings of isolation and disconnect, worsened by the physical isolation of the laboratories. Given the extreme material, DF laboratories are standalone facilities with air-gapped networks, far from regular offices.

> "We all have an idea of what an indecent image is. Of course it doesn't fully prepare you for the shock of when you first come across it." (NE)

> "I knew somebody who was literally grading with a set of rosary beads." (KH)

Participants also report using "banter as a coping mechanism" (Participant AR) and "gallows humor" (Participant PO) as outlets, "otherwise they'll end up killing themselves" (Participant KH). Dark humor is considered necessary given the work's nature ("What you say in the lab, stays in the lab," Participant TA). Participants also reported existential despair, disillusionment, and the "meaninglessness" of their job. They stated that current support and aftercare are inadequate, with Participant ZS citing that forensic units "are really good at putting an ambulance at the bottom of the cliff … but bad at stopping people from falling over."

3.4. Theme three: identifying the potential and pitfalls of automation and AI in digital forensics

This theme introduces timely concerns about the role of AI in DF that have not been extensively covered in existing research. Participants emphasized the practicality of automated images, video analysis tools, and AI algorithms in DF. These systems can automatically detect, identify, and categorize images, easing their workload across various cases, including "fraud" (Participant NE), "drug detection, grooming, and data breaches" (Participant BZ). They acknowledged that automation and AI can reduce investigator trauma, particularly in child sexual abuse cases by eliminating the need for manual grading of indecent images, especially given recent advances in welfare features being introduced into various tools (Magnet Forensics, n.d.). While these advanced tools offer significant potential for the industry, practitioners express caution, mentioning that it could also be a "hindrance" (NE), a "threat" (ZS), and "not the silver bullet" (KH), highlighting the dual nature of automation and AI in DF. Concerns include an over-reliance on these tools, unknown success rates (Participants PO, ZS, and NX), and issues in training model data regarding age and culture.

> "When we talked about indecent images and how we deal with them here in the UK compared to the kind of the bias that exists in Ghana or Albania and whether or not this is a problem or not, if all our indecent images are of Caucasian white children, and that's what the AI system is fed then it's never going to be able to grade any indecent image of a brown or a black child because it's not been taught. That and that those images don't exist because those um, the countries and you know where those would be produced because those law enforcements don't have the tools to kind of gather that information to be able to feed the system." (NE)

Participants raised concerns about the admissibility information involving the use of these tools in court and their perceived trustworthiness, credibility, and reliability. They explained that the automated tools "confirm the presence of a file. They don't explain the nature of how that file came to be" (Participant RH).

> "I mean there's … there's that trust issue, you know, have we missed something? And then I guess there's the issue of you go to court and you say, you know, "Here's the ohh, you say there's hundred images on this machine and you, but if you didn't actually do it, how are you, how are you gonna stand there and defend that? You're just gonna have to stand in court and say 'Oh, the computer did it'. So I guess the way I'd have to do it would be make it so these machines or these programs or whatever are not only trusted by the users, but trusted by courts and all that kind of stuff as well." (DM)

Participants also raised the topic of ChatGPT, the now widely-used AI chatbot, citing that it "is certainly widespread enough that our suspects are using it" (Participant PO) and that ChatGPT "will 100 % impact the forensic world" (Participant TA) in as little as six months.

3.5. Theme four: the centrality of academia in the advancement of digital forensics

Participants revealed new perspectives on academia's critical role in advancing DF, urging that "academia's biggest fallback is research" (Participant PO). "Technology is always evolving" (Participant RH), such as with mobile devices (e.g., “iOS biomes and Android versions”, Participant CL, “3500 variants of mobile phones”, Participant TA), and investigators lack the luxury of time for research. One way academic research can guide DFIs is by identifying practical methods to crack encryptions like BitLocker (de Assumpção et al., 2023). Another area participants called for focused research is on offender behavior with digital devices and concealed evidence locations:

> “Understanding perhaps where they place the most value on their collection and that can give us an indicator perhaps of where they’re hiding things, or how much encryption they put behind the things they’re trying to hide.” (PO)

Other urgent research areas participants mentioned include cloud forensics, virtual reality (VR) spaces (Participant IX), data from victims (“What can the victim give us themselves?” Participant IX), and quantum computing for breaking encryptions (“Quantum computing is essentially it,” Participant PO). This ever-evolving landscape anticipates further challenges, with criminal activity and therefore potential digital evidence sources expanding to VR spaces (Kirwan and Power, 2012), the Metaverse (Mackenzie, 2022), and smart cities (Baig et al., 2017). For instance, indecent images can be stored in VR spaces (Landi, 2023).

3.6. *Subtheme one: validation of tools as a crucial step in digital forensics*

As noted in the Introduction, tool validation is a crucial step in the digital forensic process (Tully et al., 2020). Participants found tool validation demanding, particularly due to time constraints and vendors’ unwillingness to share proprietary information.

> “I think the valid … the problem with validation is the speed at which the tech moves means that the validations are out of date by the time you’ve written it. What I think is the national … like the national requirement for … for these processes should be done by academia.” (KH)

This affects the quality of the work produced. Participants suggested involving academia (e.g., deciphering tool functionality and validating it), to ease some of the burden on DFIs while generating valuable insights. These insights would equip the DFI community to become more proficient in their work. While Participant PO acknowledged that ISO standards are well-meant and assure quality, he noted that they significantly add to their workload. Participant IX explained, “the more tools you’ve got, the more work you have to do around keeping those tools accredited,” and “a 30-minute job turning into a 2-hour job, which makes their workload harder to manage, and means they leave later and can’t switch off when they finish work” (PO). Participants advocated for implementing a standardized validation process and a “national model” (KH) to streamline validation efforts.

4. Discussion

Our analysis reveals that DFIs face considerable pressure to excel while juggling multiple roles, yet the available support remains insufficient with various unaddressed challenges impacting their work. The quality of their examination is influenced by police officers and legal professionals involved in the investigation. Additionally, the growing array of devices and spaces holding digital evidence adds further strain. Managing this volume places significant pressure on police, legal personnel, and DFIs.

This was reflected in our first finding: challenges in working with police officers dominated participants’ accounts. Officers struggle with searching, seizing, and handling digital evidence correctly, aligning with prior research (Thompson and Manning, 2021; Wilson-Kovacs, 2021). While it helpful for DFIs to accompany searches and handle evidence, this practice is either discouraged to ensure impartiality or not always possible due to logistical constraints. As a result, officers must conduct searches on their own. Crucial evidence is often at risk of loss or being omitted if not properly searched, seized, and handled by the first responder and investigating officer. This also inadvertently violates ACPO’s first principle, which emphasizes that any actions taken by police officers must not alter data to be considered admissible in court.

DFIs also serve as witnesses in court, where they are required to effectively communicate technical jargon effectively to non-technical audiences. Participants called for more training in presenting digital evidence and navigating the courtroom. Our findings also reveal that legal professionals’ generally do not understand digital evidence very well, often confusing technical terms. This can lead to evidence being arbitrarily dismissed or wrongly admitted into court. Our research extends previous work (Barysė, 2022; Belshaw and Nodeland, 2022; Hadlington et al., 2021; Kessler, 2010; Schreuders et al., 2018; Thompson and Manning, 2021; William and Humphries, 2019; Wilson-Kovacs, 2021) by providing a holistic picture where we stress the need for law enforcement and judiciary systems to improve their digital knowledge. We also underscore the need for professional rapport and increased communication between police, court personnel, and DFIs (Gabbert et al., 2021).

Third, the DFIs reported psychological and emotional trauma, and that they currently lack adequate support from their organizations and national systems. Participants described feeling distressed, disconnected, and struggling emotionally to cope. This new finding highlights the solitary nature of their work, building on Tehrani (2023). We reveal harmful work norms in this field that may cause participants to deny their trauma and internalize these negative experiences instead.

Fourth, consistent with Barysė (2022), participants were open to incorporating AI technologies to assist with certain aspects of their work. They recognized the usefulness of automation and AI in areas like initial analysis, image processing, and data extraction, particularly for grading indecent images. Tools like Griffeye, with features such as binary and visual stacking, break timers, and video sound-off by default, can help limit exposure to extreme materials (Magnet Forensics, n.d.). Nevertheless, they recommended human oversight, especially in cases where AI or automation will be used to provide evidence in court. Indeed, they striked a balance between acknowledging the potential of automation and AI in making the digital investigation process easier, while questioning the current state of its trustworthiness and explainability (XAI) to support DF (Kelly et al., 2020).

Lastly, in line with Horsman (2019), the participants called for collaboration between academic institutions and digital forensic units, urging research into critical topics in the field—echoing suggestions by Harichandran et al. (2016) and Tun et al. (2016). This collaboration can take the shape of launching forums and conversational platforms, and will equip future DFIs with evidence-based research that incorporates the latest technological advancements. Taken together, these findings reflect the dynamic challenges that digital forensic investigators in the UK face in relation to those who support their role.

5. Implications and future directions

As tabularized in Table 4, we make recommendations with an eye to the dynamic nature of DF and its status as an emerging field (Goodison et al., 2015). We propose that a shift in mindset of law enforcement personnel is needed to transform digital policing, and we suggest the development of police officers’ and court personnel’s best practice guides for digital investigations. This should span from correct searching, seizing, and handling of digital evidence through to the understanding and admittance of such evidence in court.

First, we highlight that there are currently no standardized, established protocols for first responders and police officers to search and seize digital evidence at crime scenes. This underscores a crucial gap in practice in digital policing. Equipping officers with a digital toolkit—a general checklist outlining a clear set of standardized best practices in conducting initial searches and seizing digital evidence—will ensure that frontline officers are better equipped to collect and preserve

Table 4
Recommendations and future opportunities for digital forensics in the UK.

Category	Recommendation and Future Opportunity	Details
Toolkit for Officers	Equip police officers with a toolkit for evidence collection and preservation.	Implement a checklist of standardized best practices for initial searches and evidence seizure.
Training for Legal Professionals	Enhance understanding of digital evidence among court personnel.	More training and resources for legal professionals to improve their understanding of digital evidence.
Communication Protocols	Improve communication between DFIs, police officers, and legal professionals.	Foster better professional rapport through enhanced communication protocols.
Professional and Expert Witness Training	More training and guidelines for DFIs as professional and expert witnesses.	More training opportunities for DFIs to better prepare them for court.
Psychological Support and Techniques	Implement regular psychological assessments; foster a supportive working culture; utilize psychological techniques.	Regularly assess the mental health of DFIs; Promote openness about mental health struggles; Encourage the use of psychological resources; Incorporate techniques such as cognitive behavioral strategies such as playing Tetris after work to mitigate intrusive memories.
Distress Identification	Provide line managers with indicators to identify distress.	Equip line managers with tools to recognize and address signs of distress among DFIs.
AI Trust and Transparency	Address concerns regarding AI accuracy and accountability.	Focus on improving AI fairness, explainability, and cross-cultural bias reduction to enhance trust in algorithmic decision-making.
Academic Collaboration and Emerging Technologies	Partner with academic institutions to revise DF curriculum; explore research areas; standardize validation processes.	Collaborate with academia to update curricula and work towards implementing a national validation model; Explore research areas related to new digital platforms and data acquisition methods.

evidence at the scene. Similar to what Hadlington et al. (2021) and Wilson-Kovacs (2021) suggested, onsite triaging and initial digital inquiries prior to arrival at a crime scene will help police officers gain a better understanding of the intended objectives of the particular investigation. This inquiry will also guide the officers on specific evidence to seize, what types of evidence to prioritize (such as, *only* communication from February to July between the suspect and victim of a particular year), and subsequently, how to handle the evidence correctly (such as, to pack evidence in Faraday bags or to leave computers plugged in).

Our findings also highlight legal professionals' general lack of understanding of digital evidence, and the many ways digital evidence can be acquired, as well as the many sources of digital evidence. This impacts how court personnel assess the value of digital evidence; it can also cause a domino effect in its unfair dismissal or its improper admission in court if they do not have a good grasp of its probative and prejudicial value. While providing information guidance as a toolkit is essential, it is evident that both law enforcement and legal professionals need to improve their digital skills and understanding of digital evidence. This is in line with a new set of principles proposed by Horsman (2020). Enhancing communication protocols between DFIs, police officers, and lawyers will also foster professional rapport (Gabbert et al., 2021). Currently, there is no best practice guideline for DFIs serving as expert witnesses in England and Wales. DF could draw inspiration from existing guidelines such as one set by the British Psychological Society (BPS) for psychologists serving as expert witnesses in court (British Psychological Society, 2021). Providing DFIs with a best practice guide to better prepare them for court can help to clarify their role in court either as an expert witness or witness. (We further note that there is also no directory of relevant expert witnesses to guide lawyers in the UK.)

The DF working culture must also be transformed, and several steps can be taken to achieve this. This includes enforcing more regular face-to-face psychological evaluations, alongside encouraging a culture of openness so that DFIs feel able to openly express their struggles. Other avenues to combat trauma in investigators include providing line managers with key indicators to identify distress better (Tehrani, 2023), as well as drawing from cognitive psychology research to equip DFIs with blueprints to maintain healthier emotional states, such as playing Tetris after work to prevent intrusive memories (Iyadurai et al., 2018). It is essential for DFIs to be able to refer themselves through the appropriate channels and to ensure they can access necessary assistance when needed.

Our participants revealed some hesitancy towards AI; we found some concerns regarding its accuracy and accountability for errors which affects how much trust they feel they can place on algorithmic decision-making in DF. Furthermore, the degree of trust varied depending on its application, similar to the findings of Barysė and Sarel (2023). Before placing their trust entirely in algorithmic decision-making, specific concerns require attention. For instance, to ensure fairness and to move towards explainable AI (XAI), cross-cultural biases where AI models may operate differently across diverse cultural contexts must first be addressed (Dunsin, 2023) with further implications for its application in court processes and trustworthy XAI in DF (Du et al., 2020).

Lastly, our findings indicate that DF can benefit from partnering with academic institutions. Humphries et al. (2021) and Naqvi et al. (2019) commented on the need to revise the DF curriculum to ensure that the curriculum can more effectively shape quality graduates who will possess critical thinking in the field. Our participants advocated for the implementation of a standardized validation process (rather than validation of tools) or a national model, recognizing that it can substantially systematize validation efforts. This is especially consequential when no digital forensic expert is capable of knowing and/or employing all of the forensic tools available (Batten and Pan, 2010). We anticipate new legal and policy implications for DF with the emergence of new research areas, as well as the expansion of digital devices across new platforms such as virtual worlds (viz. Metaverse) and smart cities (Baig et al., 2017; Mackenzie, 2022). Our participants suggested both industrial and legal research avenues are needed, and named upcoming areas of research such as cloud forensics and alternative methods of data acquisition (for example, data from victims themselves). Taken together, the recommendations set above will invariably impact the quality of evidence seized, promote better relationships between DFIs and police officers as well as legal professionals, and in turn enhancing the likelihood of delivering justice to victims of crime.

6. Limitations

One of our study's limitations is the low representation of females in our sample; we only had three such participants. Unfortunately, this gender imbalance is not unique to our study but mirrors a broader trend in the DF domain (Wagstaff and LaPorte, 2018). Similarly, we only had two participants who identified as non-White, reflecting low racial and ethnic diversity in our sample. All participants in this study identified as cisgender, so there was no real diversity in our sample with regard to sexual orientation either. Given this, we understand that the experiences had by participants in our sample may not fully be representative of other groups as certain unique features of other groups' experiences may not have been captured. Future research should make an effort to be more diverse in its sampling to ensure better representation of DF.

7. Conclusion

This paper explores the current challenges faced by Digital Forensic Investigators (DFIs) and future directions in England and Wales. Key findings of this novel paper include: 1) highlighting transformation in digital policing is promptly required; 2) calling for more support that is tailor-made and the development of better collaborative frameworks be available for DFIs; and 3) providing meaningful insights into the dynamic world of DF. Crucially, this paper addresses a number of different aspects of the field—including procedural, psychological, and systemic issues in combination with specialist technical aspects. As a final point, we urge vigilance in upcoming AI ethical and regulatory changes (Barysė, 2022; Kelly et al., 2020) with regard to DF.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Author's contributions

All authors contributed to the formulation of the interview schedule. Both MN and JJ conducted the interviews and analyzed the data. MN wrote the manuscript and conceptualized all figures and tables. RB edited the manuscript, and all authors (MN, JJ, and RB) reviewed the final manuscript. We would like to thank Dr. Tina Cartwright (not a named author) for her guidance and expertise in conducting a reflexive thematic analysis.

CRediT authorship contribution statement

Magdalene Ng: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Supervision, Writing – original draft, Writing – review & editing. **Jade James:** Conceptualization, Methodology, Writing – original draft, Writing – review & editing. **Ray Bull:** Supervision, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.fsidi.2024.301839.

References

Baig, Z.A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, P. K., Ibrahim, A., Sansurooah, K., Syed, N., Peacock, M., 2017. Future challenges for smart cities: cyber-security and digital forensics. Digit. Invest. 22, 3–13.

Barber, M., 2020. The First Report of the Strategic Review on Policing in England and Wales. Police Foundation (Police Foundation, London).

Barysė, D., 2022. People's attitudes towards technologies in courts. Laws 11 (5), 71.

Barysė, D., 2022. Do we need more technologies in courts? Mapping concerns for legal technologies in courts [Preprint]. https://ssrn.com/abstract=4218897. https://doi.org/10.2139/ssrn.4218897.

Barysė, D., Sarel, R., 2023. Algorithms in the court: does it matter which part of the judicial decision- making is automated? Artif. Intell. Law 1–30.

Batten, L.M., Pan, L., 2010. Testing digital forensic software tools used in expert testimony. In: Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions. IGI Global, pp. 257–278.

Belshaw, S., 2019. Next generation of evidence collecting: the need for digital forensics in criminal justice education. J. Cybersecurity Educat. Res. Pract. (1).

Belshaw, S., Nodeland, B., 2022. Digital evidence experts in the law enforcement community: understanding the use of forensics examiners by police agencies. Secur. J. 35, 248–262.

Braun, V., Clarke, V., 2019. Reflecting on reflexive thematic analysis. Qual Res Sport Exerc Health 11 (4), 589–597.

Braun, V., Clarke, V., 2021. Can I use TA? Should I use TA? Should I not use TA? Comparing reflexive thematic analysis and other pattern-based qualitative analytic approaches. Counsell. Psychother. Res. J. 21 (1), 37–47.

British Psychological Society, 2021. Psychologists as expert witnesses. Retrieved from: https://www.bps.org.uk/guideline/psychologists-expert-witnesses.

Casey, E., Schatz, B., 2011. Conducting digital investigations. Digital evidence and computer crime: forensic science. Comput. Internet 187–225.

Cellebrite, Cellebrite Official Website. https://cellebrite.com/en/home/, n.d (accessed 23 August 2024).

College of Policing, 2024. Digital intelligence and investigation – new learning modules. https://www.college.police.uk/article/digital-intelligence-and-investigation-new-learning-modules#:~:text=More%20than%2090%25%20of%20reported,the%20UK%20billions%20of%20pounds. (Accessed 19 March 2024).

Cosic, J., 2017. Formal acceptability of digital evidence. Multimedia Forensics and Security : Foundations, Innovations, and Applications, pp. 327–348.

Cummins, Flory TA., 2016. Digital forensics in law enforcement: a needs-based analysis of Indiana agencies. J. Digit Forensics Secur. Law 11 (1), 4.

de Assumpção, M.B., dos Reis, M.A., Marcondes, M.R., da Silva Eleutério, P.M., Vieira, V. H., 2023. Forensic method for decrypting TPM-protected BitLocker volumes using Intel DCI. Forensic Sci. Int.: Digit. Invest. 44, 301514.

SoK: exploring the state of the art and the future potential of artificial intelligence in digital forensic investigation. In: Du, X., Hargreaves, C., Sheppard, J., Anda, F., Sayakkara, A., Le-Khac, N.-A., Scanlon, M. (Eds.), 2020. Proceedings of the 15th International Conference on Availability, Reliability and Security. https://doi.org/10.1145/3407023.3407068.

Dunsin, D., Ghanem, M.C., Ouazzane, K., Vassilev, V., 2023. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. arXiv preprint arXiv:2309.07064.

Endicott-Popovsky, B., Horowitz, D.J., 2012. Unintended consequences: digital evidence in our legal system. IEEE Secur Priv 10 (2), 80–83.

Gabbert, F., Hope, L., Luther, K., Wright, G., Ng, M., Oxburgh, G., 2021. Exploring the use of rapport in professional information-gathering contexts by systematically mapping the evidence base. Appl. Cognit. Psychol. 35 (2), 329–341.

Goodison, S.E., Davis, R.C., Jackson, B.A., 2015. Digital Evidence and the US Criminal Justice System. RAND Corporation, Santa Monica (CA).

Grübl, T., Lallie, H.S., 2022. Applying artificial intelligence for age estimation in digital forensic investigations. arXiv preprint arXiv:2201.03045.

Hadlington, L., Lumsden, K., Black, A., Ferra, F., 2021. A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. Policing: J. Pol. Pract. 15 (1), 34–43.

Harichandran, V.S., Breitinger, F., Baggili, I., Marrington, A., 2016. A cyberforensics needs analysis survey: revisiting the domain's needs a decade later. Comput. Secur. 57, 1–13.

Holt, T.J., Clevenger, S., Navarro, J., 2020. Exploring digital evidence recognition among officers and troopers in a sample of a state police force. Policing: Int. J. 43 (1), 91–103.

Home Office, 2021. Forensic science providers: codes of practice and conduct 2021, issue 7. https://www.gov.uk/government/publications/forensic-science-providers-codes-of-practice-and-conduct-2021-issue-7. (Accessed 23 August 2024).

Horsman, G., 2017. Can we continue to effectively police digital crime? Sci Justice, 57 (6), 448–454.

Horsman, G., 2019. Raiders of the Lost Artefacts: Championing the Need for Digital Forensics Research. Forensic Science International: Reports, vol. 1, 100003.

Horsman, G., 2020. ACPO principles for digital evidence: time for an update? Forensic Sci. Int.: Report 2, 100076.

Humphries, G., Nordvik, R., Manifavas, H., Cobley, P., Sorell, M., 2021. Law enforcement educational challenges for mobile forensics. Forensic Sci. Int.: Digit. Invest. 38, 301129.

ILAC, 2022. ILAC guidance series. https://ilac.org/publications-and-resources/ilac-guidance-series/. (Accessed 23 August 2024).

Interpol, 2023. Digital forensics. https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics. (Accessed 23 January 2023).

Iyadurai, L., Blackwell, S.E., Meiser-Stedman, R., Watson, P.C., Bonsall, M.B., Geddes, J. R., Nobre, A.C., Holmes, E.A., 2018. Preventing intrusive memories after trauma via a brief intervention involving Tetris computer game play in the emergency department: a proof-of-concept randomized controlled trial. Mol. Psychiatr. 23 (3), 674–682.

James, J.I., Gladyshev, P., 2013. A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview. Digit. Invest. 10 (2), 148–157.

Jarrett, A., Choo, K.K.R., 2021. The impact of automation and artificial intelligence on digital forensics. Wiley Interdisciplin. Rev.: Forensic Sci. 3 (6), e1418.

Johnson, B.T., Riemen, J.A., 2019. Digital capture of fingerprints in a disaster victim identification setting: a review and case study. Forensic Sci. Res. 4 (4), 293–302.

Kelly, L., Sachan, S., Ni, L., Almaghrabi, F., Allmendinger, R., Chen, Y., 2020. Explainable artificial intelligence for digital forensics: opportunities, challenges and a drug testing case study. Digital Forensic Sci.

Kessler, G.C., 2010. Judges' Awareness, Understanding, and Application of Digital Evidence [dissertation]. Fort Lauderdale (FL). Nova Southeastern University.

Kessler, G.C., Carlton, G.H., 2020. Exploring myths in digital forensics: separating science from ritual. In: Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice. IGI Global, pp. 355–364.

Kirwan, G., Power, A., 2012. Crime in virtual worlds: should victims feel distressed?. In: The Psychology of Cyber Crime: Concepts and Principles. IGI Global, pp. 212–226.

Landi, M., 2023. Virtual reality could be used to treat sex offenders who abuse children. Independent. https://www.independent.co.uk/news/uk/home-news/sex-offenders-virtual-reality-abuse-children-b2404874.html.

Lawton, D., Stacey, R., Dodd, G., 2014. eDiscovery in Digital Forensic Investigations. CAST Publication, 32/14.

Mackenzie, S., 2022. Criminology towards the Metaverse: cryptocurrency scams, grey economy and the technosocial. Br. J. Criminol. 62 (6), 1537–1552.

Magnet Forensics, 2023. Magnet Griffeye user wellbeing features. https://www.magnetforensics.com/resources/magnet-griffeye-user-wellbeing-features/. (Accessed 5 August 2024).

Marshall, A.M., 2010. Quality standards and regulation: challenges for digital forensics. Measurem. Control 43 (8), 243–247.

McEwen, A., 2021. Computer found in room of Scots terror plan accused "held 1000s of hate images." Daily Record. Available from: https://www.dailyrecord.co.uk/news/scottish-news/computer-found-bedroom-scots-terror-25216152.

Miller, C.M., 2023. A survey of prosecutors and investigators using digital evidence: a starting point. Forensic Sci. Int. Synergy 6, 100296.

Montasari, R., 2017. Digital evidence: disclosure and admissibility in the United Kingdom jurisdiction. In: Global Security, Safety and Sustainability-The Security Challenges of the Connected World: 11th International Conference, ICGS3 2017; 2017 Jan 18-20; London, UK. Springer International Publishing, New York, pp. 42–52.

Montasari, R., Hill, R., 2019. Next-generation digital forensics: challenges and future paradigms. In: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3); 2019 Jan; London, UK. IEEE, New York, pp. 205–212.

Morris, S., Hadgkiss, M., David, A., Guinness, J., Frewin, C., 2023. We're making a list and we're checking it twice, gonna find out what makes digital forensic examiners suffice. Wiley Interdisciplin. Rev.: Forensic Sci. 5 (5), e1487.

MSAB, MSAB Official Website. https://www.msab.com/, n.d. (accessed 23 August 2024).

Naqvi, S., Sommer, P., Josephs, M., 2019. A research-led practice-driven digital forensic curriculum to train next generation of cyber firefighters. In: 2019 IEEE Global Engineering Education Conference (EDUCON); 2019 Apr; Dubai, UAE. IEEE, New York, pp. 1204–1211.

National Police Chiefs' Council (NPCC), 2020. National digital forensic science strategy. Retrieved from. https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/2020/national-digital-forensic-science-strategy.pdf.

Page, H., Horsman, G., Sarna, A., Foster, J., 2019. A review of quality procedures in the UK forensic sciences: what can the field of digital forensics learn? Sci. Justice 59 (1), 83–92.

Piper, M., 2023. Witnessing a Gap: How Digital Forensic Expert Witness Qualifications Differ from Attorney Expectations [doctoral Dissertation]. Purdue University, West Lafayette.

Police Digital Service (PDS), 2022. Transforming forensics. https://pds.police.uk/tag/transforming-forensics/. (Accessed 4 April 2023).

Pollitt, M., 2010. A history of digital forensics. In: Advances in Digital Forensics VI: Sixth IFIP WG 11.9 International Conference on Digital Forensics; 2010 Jan 4-6; Hong Kong, China. Springer Berlin Heidelberg, Berlin, pp. 3–15.

Regional Organised Crime Units, 2024. Serious and organised crime disruption across regions. https://www.rocu.police.uk/. (Accessed 24 August 2024).

Regulation of Investigatory Powers Act, 2003 (Chapter 23). The Stationary Office, London. https://www.legislation.gov.uk/ukpga/2000/23/contents. (Accessed 13 February 2024), 2003.

Sammons, J., 2014. The Basics of Digital Forensics: the Primer for Getting Started in Digital Forensics. Syngress.

Schreuders, Z.C., Cockcroft, T., Butterfield, E., Elliott, J., Soobhany, A.R., Shan-A-Khuda, M., 2018. Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force (Unpublished).

Slay, J., Lin, Y.C., Turnbull, B., Beckett, J., Lin, P., 2009. Towards a formalization of digital forensics. In: Advances in Digital Forensics V: Fifth IFIP WG 11.9 International Conference on Digital Forensics; 2009 Jan 26-28; Orlando, FL, USA. Springer Berlin Heidelberg, Berlin, pp. 37–47.

Sokol, P., Rózenfeldová, L., Lučivjanská, K., Harašta, J., 2020. IP addresses in the context of digital evidence in the criminal and civil case law of the Slovak Republic. Forensic Sci. Int.: Digit. Invest. 32, 300918.

Solon, M., 2019. The times bond Solon expert witness survey 2019. Int'l In-House Counsel J 12, 1.

Sommer, P., 2011. Certification, registration and assessment of digital forensic experts: the UK experience. Digit. Invest. 8 (2), 98–105.

Sunde, N., Dror, I.E., 2019. Cognitive and human factors in digital forensics: problems, challenges, and the way forward. Digit. Invest. 29, 101–108.

Tehrani, N., 2023. The Role of Psychological Surveillance in Reducing Harm and Building Resilience in Police Forensic Investigators. Police J, 0032258X231151996.

The Independent, 2023. BTK killer Dennis Rader's daughter says it's possible her father committed two additional murders. https://www.independent.co.uk/news/world/americas/crime/btk-killer-dennis-rader-kerri-rawson-b2401889.html. (Accessed 21 August 2024).

Thompson, P., Manning, M., 2021. Missed opportunities in digital investigation. In: Cybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability; 2021 Jan ; Virtual. Springer International Publishing, Cham, pp. 101–122.

Tully, G., Cohen, N., Compton, D., Davies, G., Isbell, R., Watson, T., 2020. Quality standards for digital forensics: learning from experience in England & Wales. Forensic Sci. Int.: Digit. Invest. 32, 200905.

Tun, T., Price, B., Bandara, A., Yu, Y., Nuseibeh, B., 2016. Verifiable limited disclosure: reporting and handling digital evidence in police investigations. In: 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW); 2016 Sep; Beijing, China. IEEE, New York, pp. 102–105.

UKAS, UKAS Official Website. https://www.ukas.com/, n.d. (accessed 23 September 2024).

Vincze, E.A., 2016. Challenges in digital forensics. Police Pract. Res. 17 (2), 183–194.

Wagstaff, I.R., LaPorte, G., 2018. The importance of diversity and inclusion in the forensic sciences. Nation. Instit. Justice J. 279, 81–91.

Williams, J., Humphries, G., 2019. Public Understanding of Cyber Security and Digital Forensics within the UK.

Wilson-Kovacs, D., 2021. Digital media investigators: challenges and opportunities in the use of digital forensics in police investigations in England and Wales. Policing: Int. J. 44 (4), 669–682.