

Article

An ‘Enlightenment Phase’: Police Perspectives on the Contemporary Challenges of Digital Evidence and Digital Forensic Investigations

Magdalene Ng ^{1,*} , Rachael Medhurst ²  and Coral J. Dando ¹ 

¹ Psychology, School of Social Sciences, University of Westminster, 115 New Cavendish St., London W1W 6UW, UK; c.dando@westminster.ac.uk

² Faculty of Computing, Engineering and Science, University of South Wales, Newport NP20 2BP, UK; rachael.medhurst@southwales.ac.uk

* Correspondence: ngm1@westminster.ac.uk

Abstract

Digital evidence (DE) continues to evolve alongside rapid technological innovation, including the increasing integration of AI-generated media, algorithmic tools, and digital forensic technologies used to identify, extract, and analyse digital artefacts in criminal investigations. Yet, limited work has examined how frontline police officers interpret and operationalise digital forensic outputs, particularly in the context of emerging forms of AI-mediated evidence. We investigated the perceptions of 13 police officers in England and Wales regarding the evolving role of DE and digital forensic investigations, and the implications for policing practice. Reflexive thematic analysis identified four themes: (i) AI and the evolving landscape of digital forensic investigations; (ii) digital systems and the infrastructure of investigations; (iii) human judgement and trust in the interpretation of DE; and (iv) building digital expertise in modern investigations. Participants described a marked rise in highly realistic AI-generated imagery, which complicates evidence categorisation and proportionality assessments. This also reshapes investigative decision-making while necessitating adaptations in investigative interviewing, particularly around disclosure sequencing and evidential challenge. Findings suggest that understanding of AI and algorithmic systems among some frontline officers remains underdeveloped, raising concerns about the interpretation of outputs. By foregrounding practitioner perspectives, this study contributes a human-centric understanding of digital forensic practice, while offering insights into the future development of investigative approaches in response to emerging technologies and evolving threats.

Keywords: digital evidence; digital forensics; human factors; digital forensic investigations; AI-generated evidence



Academic Editors: Jing-Wein Wang,
Malinka Spasova Ivanova, Galina
Bogdanova and Tomaž Klobučar

Received: 26 March 2026

Revised: 6 May 2026

Accepted: 22 May 2026

Published: 1 June 2026

Copyright: © 2026 by the authors.
Licensee MDPI, Basel, Switzerland.
This article is an open access article
distributed under the terms and
conditions of the [Creative Commons
Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Digital evidence is now foundational to modern policing. The term Digital Evidence (henceforth referred to as “DE”) refers to any data generated, stored, or transmitted within digital devices or online systems that may be relevant for criminal investigation purposes [1]. Examples of such data include individual digital traces, which are discrete artefacts such as text messages, photographs, GPS logs, CCTV footage, cloud account records, application data, body-worn camera files, and cryptocurrency transactions, all of

which may help investigators to reconstruct events in question [2]. Most criminal investigations now involve some form of a digital trail or trace information [3–7] and are increasingly associated with complex and technologically mediated forms of data. However, as digital traces grow in scale and sophistication, the challenge is no longer only in recovering data, but in determining what can be trusted as a reliable representation of events.

DE is different from traditional forms of evidence in several important respects. First, it is inherently more fragile and volatile in comparison to physical traces such as DNA or fingerprints [2]. Digital data can be encrypted, remotely deleted, edited, or overwritten—all of which limits their recoverability [8,9]. It also does not appear in only one form. It can be distributed bit-for-bit, identically copied, and is not tied to one physical object [2]. Added to this, the sheer volume and variety of DE sets it apart from other types of evidence [10]. Compared to a strand of hair, a tiny physical space can hold terabytes of data [2]. Access is further complicated by digital forensic backlogs or legal barriers in obtaining data and platform records [4,11,12].

Digital forensic investigations typically involve the identification, collection, preservation, extraction, and analysis of digital artefacts recovered from electronic devices, platforms, and networked systems [13]. Through specialised tools and procedures, practitioners known as digital forensic investigators recover and analyse digital artefacts that may be relevant to reconstructing events, identifying suspects, or corroborating witness accounts [13].

To note, the work of digital forensic specialists represents only one stage of the investigative process. Digital forensic investigators focus primarily on the technical recovery and analysis of data; once digital material has been extracted or analysed, police investigators must interpret these outputs, integrate them with other forms of evidence, and use them to guide investigative decisions, interviews, and charging decisions [13]. In other words, police investigators are responsible for interpreting the meaning, relevance, and reliability of digital artefacts within the broader investigative context. Understanding how police officers interpret and make sense of DE is therefore critical, as investigative outcomes ultimately depend not only on the technical recovery of digital data but also on how this information is evaluated and used during criminal investigations [13].

The increasing reliance on digital forensic technologies in criminal investigations has transformed the way investigators identify, collect, and analyse DE from devices, platforms, and networked environments. These include mobile device extraction systems, forensic imaging tools, and automated image classification tools designed to assist investigators in processing large volumes of digital data. Recent developments in policing demonstrate a clear shift towards automation, scalability, and Artificial Intelligence (AI)-assisted analysis to help investigators manage the growing volume and complexity of DE more efficiently [14].

1.1. Related Work

Despite DE playing a central role in shaping investigative processes [15–17], organisational challenges remain within digital forensic practice. Research highlights issues such as resource limitations, backlogs, and variability in digital expertise across policing contexts [7]. Frontline officers have been found to report feeling underprepared to manage cyber-enabled crime [18], and studies suggest that digital investigative opportunities are missed in a substantial proportion of serious crime investigations [19,20].

Beyond organisational challenges, digital traces are inherently interpretative artefacts, whose meaning is constructed through inferential judgments about the activity that produced them [21]. For example, investigators must interpret chat logs not just as raw strings of text, but in terms of meaningful content, conversational structure, intent, and context, since relevance to a case often depends on establishing whether specific interac-

tions demonstrate purposeful behaviour or patterns associated with criminal activity [22]. More broadly, research on investigative reasoning demonstrates that decision-making in criminal investigations has always involved interpreting evidence under conditions of uncertainty [23]. Within digital contexts, these cognitive demands are amplified, as officers must interpret complex and often ambiguous digital artefacts alongside other forms of evidence.

Meanwhile, DE continues to evolve rapidly. Advances in AI-generated media and automated analytical systems are reshaping how digital artefacts are produced, analysed, and interpreted [9,10]. These developments introduce new challenges relating to authenticity, reliability, and evidential interpretation, further increasing the demands placed on investigators.

1.2. Present Study and Contributions

Despite the accelerated evolution of DE, most digital forensic research has traditionally focused on technical extraction and analytical methods [10,13]. Less attention has been paid to how frontline police investigators interpret and use digital forensic outputs within investigative decision-making, as well as how they anticipate DE developing in practice. As DE becomes increasingly ubiquitous, understanding how law enforcement navigates shifting crime patterns, technological complexity, and evidential uncertainty is critical. Interpretation of DE is becoming more complex and often ambiguous with a growing reliance on human judgment and investigative reasoning to determine authenticity, attribution, and evidential value. There are various challenges within DE such as the growing volume of data, heterogeneity, volatility of DE, as well as the increasing integration of AI within case work, both within criminality and within digital forensic tools.

With all of this in mind, the present study examines how frontline police officers perceive the evolving nature of DE and the field of digital forensics, with a particular focus on the human factors shaping how they understand its future trajectory and implications for criminal investigations. Specifically, it examines how police officers in England and Wales conceptualise the evolving landscape of DE, the risks and ambiguities it generates, and highlights the recommendations they consider necessary. The study addresses two research questions:

- (1) How do police officers conceptualise the evolving nature of DE?
- (2) What emerging challenges and potential recommendations do officers identify for future digital investigations?

2. Methodology

2.1. Participants

$N = 13$ police officers from forces across England and Wales were recruited using a combination of snowball and expert sampling. Participants were individual officers working across multiple police forces, including the Metropolitan Police Service, British Transport Police, Thames Valley Police, West Midlands Police, and Greater Manchester Police. The sample included 11 male and two female officers, all with varied experience levels, among them several digital media investigators. The sample of 13 officers enabled rich exploration of investigative perspectives and sufficient diversity of experience to support the development of robust themes, consistent with reflexive thematic analysis [24]. Participant profiles are summarised in Table 1, where some demographic information were not disclosed by all participants. The average age was 39.1 years, ranging from 22 to 53 years of age. The mean length of police service was 14 years and 10 months, ranging from 1 year 9 months to 29 years of service.

Table 1. Participant profiles.

Pseudonym	Age	Gender	Rank/Role	Years of Service
BL	34	Male	Police Constable (soon Sergeant)	~11 yrs
MS	50	Male	Police Sergeant	~10 yrs
GO	53	Male	Detective Sergeant	~29 yrs
WS	38	Male	Digital Media Investigator	5 yrs 3 mos
JK	–	Male	Digital Media Investigator	~20 yrs
SK	49	Male	Digital Media Investigator	~29 yrs
CL	–	Male	Detective Sergeant	20 yrs 3 mos
RP	–	Male	Detective Chief Inspector	22 yrs 7 mos
CD	22	Female	Police Constable	1 yr 9 mos
DB	36	Male	Detective Constable	~13 yrs
IP	–	Male	Detective Sergeant	~9 yrs
TS	28	Female	Police Constable	3 yrs 5 mos
NC	42	Male	Detective Sergeant	~19 yrs

2.2. Procedure

Prior to interviews, participants provided informed consent after reading an information sheet outlining the aims of the study, their right to withdraw, and assurances of confidentiality and anonymity. Interviews were audio-recorded with consent and conducted by the first author via Microsoft Teams. The data analysed in this article were drawn from a qualitative study involving semi-structured interviews with UK police officers examining DE practices in investigations [5]. During transcription, pseudonyms were assigned to protect participants' anonymity and all further identifying information were removed. Interview durations ranged from 33 min and 53 s to 1 h 31 min and 42 s ($M = 1\text{ h }8\text{ min and }43\text{ s}$). Following each interview, participants received a written debrief and contact details for the research team. No financial incentives were offered.

2.3. Materials and Data Analysis

Participants were asked how they saw digital forensics to evolve in the coming years and whether they had recommendations for improving how DE is handled in investigations, as well as broader recommendations for the field of digital forensics. Follow-up prompts were used to encourage elaboration. This approach is consistent with reflexive thematic analysis, which supports flexible interviewing and iterative engagement with insights in the data [25,26]. After transcription, interview data were analysed using reflexive thematic analysis, following the stages outlined by Braun and Clarke [27]. This process was an iterative one which involved many rounds of coding, reviewing, and refining. Reflexive thematic analysis does not aim for agreement between multiple coders but instead recognises the researcher's active role in interpreting the data. Concepts such as data saturation, member checking, and negative case analysis were not applied, as these approaches are not typically undertaken in reflexive thematic analysis. Instead, the focus was placed on the depth and richness of the data and the quality of the analysis. Rigour was further achieved through careful, transparent, and reflective engagement with the data. Participant accounts were coded inductively (where no hypotheses were proposed at the start of the study) and informed the development of themes presented in Section 3. NVivo 15 was used to manage coding and organise the dataset, and a reflexive statement is included in Appendix A.

2.4. Ethical Considerations

Ethical approval for this study was obtained from the University of Westminster Research Ethics Committee [ETH2425-0936]. All participants provided informed consent prior to participation and were informed of their right to withdraw. To ensure confidentiality, all identifying information was removed from the data and participants were given pseudonyms. Given the sensitive nature of policing work, care was taken not to include any details that could identify individuals or specific cases. All data were stored securely in line with institutional and data protection guidelines, and only the research team had access to them.

3. Results

Four key themes were identified, illustrating how participants understood the challenges, risks, and potential reforms associated with future digital investigations. They are: (i) AI and the evolving landscape of digital forensic investigations, (ii) digital systems and the infrastructure of investigations; (iii) human judgement and trust in the interpretation of DE, and (iv) building digital expertise in modern investigations. Figure 1 illustrates the thematic map, with findings demonstrating the rapidly evolving nature of DE within contemporary investigations. These developments reflect broader transformations in digital forensic practice, where investigators must navigate increasingly complex digital environments while attempting to identify and interpret relevant evidence.

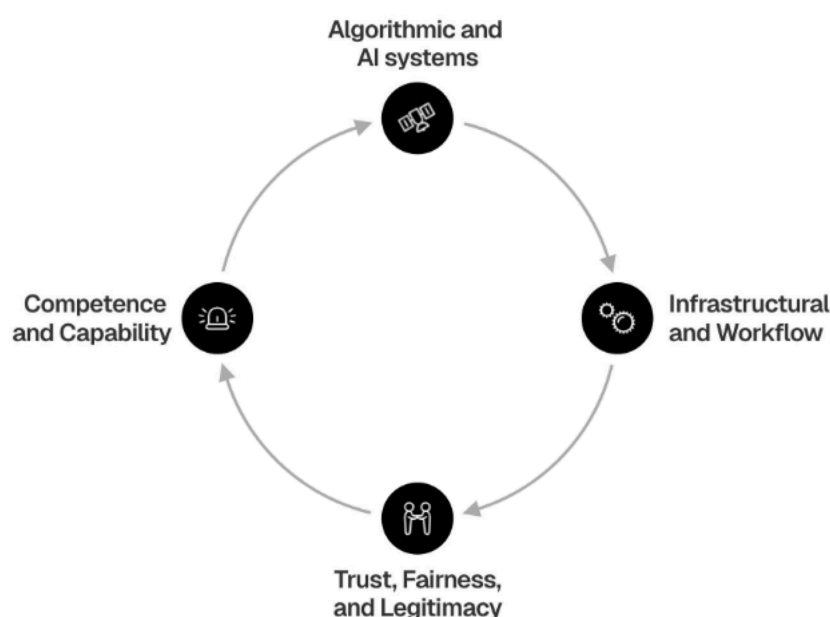


Figure 1. Thematic map of DE in contemporary policing.

3.1. Theme One: AI and the Evolving Landscape of Digital Forensic Investigations

This theme highlights the central role of investigator judgement, cognitive processing, and sense-making within an increasingly complex investigative landscape. Participants described the embedding of algorithmic and artificial intelligence (AI)-assisted systems within routine policing practice. TS mentioned the expansion of “facial recognition cameras” in central London, while MS described “blockchain” technology (which can incorporate machine learning techniques) being used to detect suspicious behaviour in financial crime and cybercrime investigations.

CD explained unmanned aircraft systems (UASs), also known as drones, to have become routine in investigations. UASs are digitally enhanced surveillance systems that capture live video, thermal imaging, geolocation, movement patterns and sometimes

incorporate AI-assisted image analytics [28]. They are useful in missing persons cases, public order, and important for border patrol [29]:

“We use drones a lot. . . hidden little cameras in the bushes next to the tracks. . . you can see exactly if someone’s hiding a mile down the tracks.” (CD)

While the benefits of these technologies are acknowledged, participants also raised risks and struggles in classifying and interpreting new digital artefacts. Synthetic and manipulated media, including deep-fake images and videos, were described as posing an emerging evidential challenge. Officers working in child abuse investigations described an “explosion of AI” (CL) in their caseloads.

Generative Adversarial Networks (GANs), diffusion-based image models, LLM-driven conversational agents [30–32] and now multimodal models [33,34], enable the large-scale production of synthetic visual and textual content. Participants noted cases of synthetic grooming where offenders increasingly use AI chatbots designed to simulate children, allowing them to rehearse sexual conversations, test boundaries, or practice manipulation strategies without interacting with real minors:

“We have offenders using AI to generate indecent images or have conversations of an indecent nature with a computer.” (CL)

Offenders also combine real photographs of minors with AI-generated or AI-altered content to sexualise, threaten, or coerce a child. This produces hybrid images in which “AI has removed clothing” (CL) of an existing photo to create the appearance of nudity. Together, this undermines assumptions about the authenticity and reliability of digital visual and audio material, while placing greater demands on the cognitive and interpretive work involved in assessing DE. Officers emphasised the increasing difficulty in knowing whether a digital material is genuine, if it has been manipulated, and if it can reliably be attributed to a suspect:

“We have to determine is that a live victim, a historical image, or an AI-generated image?” (CL)

“We’re going to struggle to identify what’s AI and what’s real life.” (TS)

Investigators must now determine whether an image depicts a real child, a fully synthetic creation, or a hybrid in which AI has altered a genuine image. This distinction matters because determining what type of image is involved has direct consequences for charging decisions and for assessing risk to actual victims.

Finally, officers anticipated an emerging “AI against AI” landscape in which policing uses AI to counter AI-enabled offending, akin to Burton et al. [35]. TS, for example, described “AI will be developed to help identify AI things”.

“AI in advanced analytics tools. . . are improving. . . the police’s ability to analyse these blockchains at large scale. . . [and] help police identify suspicious activity.” (MS)

Notably, participants in this study did not consistently distinguish between different forms of AI, often referring to them interchangeably. In this study, the term “AI” is used in the broad sense to refer to both generative AI systems (such as those used for deepfakes and synthetic media generation) and machine learning-based analytical systems (including automated detection, classification, and pattern recognition approaches) applied within digital forensic and investigative contexts. Automated workflows will be discussed in Section 3.2.

3.2. Theme Two: Digital Systems and the Infrastructure of Investigations

Across interviews, participants described the introduction of digitally automated evidence workflow systems that are reshaping how DE is captured, preserved, and trusted even before it is interpreted by officers or courts. These developments illustrate how digital forensic workflows and evidence pipelines are increasingly embedded within frontline investigative systems. For example, DB mentioned Flex, a British Transport Police (BTP) application that allows officers to photograph potential evidence, automatically log it as an exhibit, upload it directly to the case file, and record suspect interviews within the same system:

“From their phone, they’re able to take pictures. . . exhibit it directly into the case file. . . hit record and start your suspect interview.” (DB)

Alongside Flex, participants described the development of further applications designed to streamline forensic and Scenes of Crime Officer (SOCO) requests. As DB explained, “Right now we’re creating a new app where it’s a one stop shop for officers to be able to do SOCO requests”. BL noted that “remote file transfer or DE acquisition” is becoming increasingly common, reflecting a move toward digital-first processes. These examples show how digital workflows are moving onto frontline mobile devices, bringing chain-of-custody and case-building processes much earlier into police work.

Participants also described widespread fragmentation across forces, legacy IT systems, and incompatible vendor platforms. As WS noted, “old systems don’t talk to new systems,” while DB observed that digital cases may be lost because frontline officers “don’t know what they’re doing.” Similar to findings by Belshaw and Nodland [36], NC characterised the national landscape as “piecemeal and fragmented. . . almost a postcode lottery.” Participants emphasised that investigations now depend not only on officers’ skills but on an end-to-end protocol under a centralised governance to ensure a more consistent approach across forces and agencies. As NC explained, evidence must be managed “from it being seized all the way through to being interpreted, analysed” and without processes that “cover the lot,” standards lose meaning.

Participants also described shrinking data access windows, where “companies are trying to hold less data. . . they just up sticks and hide behind some international legal boundary” (JK). He illustrated the consequences using vehicle telematics:

“Four years ago. . . I’d have a granular GPS trail since the vehicle left the factory. Now you’re only going to get 24 h. . . then it just drops off.” (JK)

These accounts showed that time pressure in digital investigations are progressively shaped by changing structural systems such as data minimisation policies, platform design, and legal jurisdiction. Even when police act lawfully, access is restricted by geography:

“A lot of the tech companies will adhere to the law of the land where their data is held. . . Apple data is on US soil, so they’ll adhere to US law, not UK law.” (CL)

Taken together, this theme shows that access to and usage of DE now depends on changing infrastructures. Increasingly, platform design and data-retention policies shape what evidence exists and what survives. Crucially, much of this infrastructure lies outside the direct control of frontline policing, and yet DE is only as reliable as the end-to-end systems that carry it. Beyond individual tools, findings in this theme also point to challenges in validating end-to-end digital forensic systems. Forensic science requires not only tool validation but also validation of workflows, including acquisition, processing, storage, and interpretation. Where systems are fragmented, proprietary, or poorly understood by users, it becomes difficult to demonstrate compliance with established forensic science principles such as repeatability, reproducibility, and auditability [13].

3.3. Theme Three: Human Judgement and Trust in the Interpretation of DE

Theme Three highlights the importance of human judgement, trust, and interpretive expertise in digital forensic evidence evaluation. Participants emphasised that the legitimacy of these evolving practices depends on whether they are perceived as fair, proportionate, and trustworthy. Fairness was frequently framed in terms of proportionality, with proportionality being a principle of using the least intrusive method necessary to achieve an investigative aim. For example, MS stressed that device examinations should focus only on information genuinely relevant to the case:

“Why would I look at a drug dealer’s photos?” (MS)

Here, officers recognised that mobile phones contain highly personal material unrelated to alleged offences, and that over-collection risks both evidential overload and a perception of intrusion. Similar concerns were raised in relation to surveillance technologies, including live and retrospective facial recognition systems, where surveillance systems may be perceived as disproportionate, particularly in public spaces:

“Cameras in operation 24/7... constantly looking at people’s faces... picking up features to link them to outstanding suspects.” (TS)

Even highly accurate AI systems can undermine effective policing if they make people feel alienated or unfairly treated [37]. From a theoretical perspective, this raises questions of legitimacy, which is understood as the perception that police actions are fair, justified, and deserving of public support [38].

Where the authenticity of digital material is ambiguous, proportionality assessments become more contested [21]. Officers described growing uncertainty about how investigative responses can be justified, describing it as “moving into a grey area” (CL). For example, in CSAM cases, if no identifiable child appears to be involved, the justification for intrusive measures, such as full device examinations or arrest, may be questioned. This tension places officers in a difficult position, where decisions must not only be legally defensible, but publicly and institutionally legitimate. Courts and the public may also struggle to interpret what these images represent evidentially, creating further challenges for the perceived legitimacy of digital investigation responses.

Beyond public and community trust in digital policing, participants also described their own trust in the digital tools they use. This concerns whether officers themselves understand, question, and appropriately rely on the digital systems they use. The excerpts below suggest that facial recognition outputs may sometimes be interpreted as conveying high levels of evidential certainty, even though such systems typically produce similarity scores indicating the degree of resemblance between two facial images rather than probabilities of identity [39]:

“What about when someone doesn’t identify the person, what do we do next? Put the photo through facial recognition technology... it’s about 98% accurate.” (MS)

“Even if you don’t recognise a suspect, the footage is normally good enough to get an ID from it... 80% match, here’s your guy and it’s like ‘oh my God’.” (CD)

These accounts illustrate how investigators must interpret and evaluate algorithmic outputs in practice, wherein the evidential value of DE in part depends on how human decision-makers interpret these outputs, assess their reliability, as well as integrate them into investigative narratives. Furthermore, participants highlighted concerns about the reliability and reproducibility of digital forensic outputs. As IP noted, “different tools produce different results... even the same software but different versions... it yields

slightly different results.” This variability challenges assumptions that digital systems provide objective and stable results, as described in Horsman [40].

This theme shows that DE risks losing public (and victim confidence) because it is becoming harder to justify, explain, and defend. These observations further reflect a broader tool validation problem within digital forensics [41]. Unlike more mature forensic disciplines, where methods undergo extensive empirical validation, peer scrutiny, and are associated with clearly defined error rates, many digital forensic tools and AI-enabled systems lack comparable levels of rigorous independent validation. This is partly due to the rapid pace of technological development, the proprietary nature of many forensic software solutions, and the continual release of updated algorithms, all of which make sustained, standardised testing and reproducibility difficult to achieve in practice.

3.4. Theme Four: Building Digital Expertise in Modern Investigations

Participants agreed that current training, standards, and national infrastructure are nowhere near sufficient for the digital demands of modern policing, with current training described as “sheep dip” (GO). Others point out that College of Policing products quickly become “out-of-date” (SK). A recurring concern is the lack of foundational digital skills in officers’ careers. According to SK, “front-line especially and CID do not get inputs” into acts and legislations and that “every single force interpreted it differently” (SK). This results in uneven capability across forces, where “every single force interpret [available legislations] differently” (SK).

“If I was to wave a magic wand, I think there should be greater input at the very start of an officer’s career... it should be fundamental like legislation. Every officer should have capability to conduct digital investigations.” (SK)

This includes the growing area of open-source investigation (such as those employed by Bellingcat), which calls for specialised training and ethical literacy. Officers urged that OSINT training be incorporated as part of digital investigations:

“Every new officer should be open-source trained from day one.” (SK)

“There’s going to be much more of this [open source investigations]... it’s getting bigger and actually I can find someone without using any police systems at all, just using the Internet.” (WS)

OSINT literacy and training are important, as participants cautioned that OSINT is increasingly polluted by misidentification and manipulation. This raises the need for verification practices, provenance awareness, and auditability. WS gave the example of “doxxing... the releasing personal documents about someone to... out who they are” to illustrate this point, saying that “just because I can do something doesn’t mean I should” (WS).

Participants further drew attention to gaps in training around the communication of DE in court. GO described the complexity of presenting cell-site and movement data visually, such as overlaying datasets from multiple providers and constructing a coherent narrative for a jury:

“You would get the data from Sky... from O2... plot it on a map... overlay the data... so you can visually see what it looks like.” (GO)

This example illustrates that digital literacy also calls for the ability to translate complex data into clear, accurate courtroom explanation. Without consistent and up-to-date national training on how to interpret, visualise, and narrativise DE, officers risk miscommunicating findings, losing juries, or inadvertently overstating or understating evidential significance. As MS reflected, “How do you translate that down to officers down on the floor?” This

question reflects a broader concern that developments in digital tools and legislation are moving faster than frontline officers can keep up with.

Taken together, this theme suggests that in the absence of national training pathways, DE work can become uneven, error-prone, and difficult to defend. This is especially important and timely because participants repeatedly explain that there is a “lack of understanding and awareness” of DE (MS), making them feel like they are “always behind” (DB). NC compared current practice to an earlier era in physical forensics:

“Our digital IQ is low. I kind of liken it to. . . physical forensics, so like 80 years ago, people didn’t know anything about DNA, didn’t know much about fingerprints. And then when people did know about fingerprints and DNA to start with the technology wasn’t there. So even though we knew about it we couldn’t access it because we couldn’t make sense of it. It’s the same with digital now, we’re in that during that kind of the Enlightenment phase.” (NC)

4. Discussion

This study examined how police officers in England and Wales interpret and make sense of DE within increasingly complex digital forensic investigations. Digital forensic research has traditionally focused on the technical extraction and analysis of digital artefacts [10,13,41]. Together, these themes illustrate that the interpretation of DE is equally shaped by human judgement, investigative reasoning, and contextual knowledge. Understanding how investigators interpret, trust, and challenge digital forensic outputs therefore represents an important human-factors dimension of digital forensic practice.

Theme one: At the heart of Theme One lies the finding that generative AI and machine learning-based systems are reshaping the conditions under which DE is produced, interpreted, and defended. Many contemporary investigative systems now incorporate algorithmic and machine learning tools designed to assist in analysing large digital datasets. As cases involving AI-generated imagery become more widespread, investigators face growing demands to distinguish between live victims, historical abuse, fully AI-generated content, and hybrid material. This directly affects harm assessment, charging decisions, sentencing, and victim identification. Although UK indecent image offences encompass “pseudo-photographs,” and realistic depictions are treated as indecent images under the Protection of Children Act 1978, clearly non-realistic imagery falls within the “prohibited images” provisions of the Coroners and Justice Act 2009. Highly realistic AI-generated material blurs this legal boundary, as age and victim status may need to be inferred from appearance rather than linked to an identifiable child [42,43]. Extending Thompson and Manning’s [20] discussion of digital investigative gaps, our findings suggest that DE is becoming increasingly difficult to categorise and authenticate even when they do use digital lines of enquiry. At present, there is no standardised national framework for identifying AI-generated CSAM and deepfakes in the UK. Detection relies on visual inspection, metadata analysis, and specialist tools [44]. Regulatory reforms, including the UK Online Safety Act 2023 [45] and the EU Digital Services Act [46] strengthen platform duties to detect and remove illegal content. However, these frameworks do not fully resolve the evidential classification or interpretation of AI-generated material. While relevant legal frameworks are evolving, they do not yet provide clear operational guidance for evidential classification, attribution, or interpretation of AI-generated material, leaving significant discretion to investigators and courts, which aligns with participants accounts of increasing ambiguity in evidential categorisation and decision-making. Some forces have begun developing internal policies and national advisory groups are providing some expertise [47,48], yet the absence of national standards places greater cognitive and interpretive demands on investigators (and courts) in evaluating the authenticity, attribution, and intent of such material.

Indeed, where no real victim can be identified, liability may depend on whether the suspect knew, intended, or was reckless as to the depiction of a child. Where suspects claim a lack of knowledge, control, and deliberate engagement (e.g., “It wasn’t me, AI generated it”; “It just appeared”; “I was role-playing with a bot”), detailed questioning about installation, prompt use, file saving, and repeated generation can become central. This may also require strategic use of DE during interviews, particularly in how evidence is disclosed and used to challenge inconsistencies in suspects’ accounts.

Participants described an ongoing “AI fighting AI” arms race, despite tools being available to detect manipulated media [35,44]. First, this framing of “AI fighting AI” highlights a degree of conceptual ambiguity, suggesting that frontline understanding of AI is underdeveloped. This in turn may shape how such tools are interpreted, trusted, and operationalised in practice. Second, as generative systems advance, detection becomes less certain and more probabilistic. Increased uncertainty undermines confidence in DE, requiring officers, courts, and victims to navigate greater ambiguity [21]. Victims may fear not being believed [49], suspects and lawyers may contest authenticity, courts must weigh expert uncertainty, and officers must justify their conclusions. We will further expound on these issues in Theme Three.

Theme two: This theme shows that digital workflows are already moving onto frontline mobile devices, where frontline officers are now having to upload evidence and initiate forensic requests digitally. DE is now handled by a wider range of officers, rather than being confined to specialist digital forensic teams. The introduction of technical responsibility for officers also increases the potential for procedural error and new points of vulnerability. Especially where participants described governance gaps, and where officers do not fully understand how these processes align with forensic standards.

This shift in responsibility may increase cognitive workload and affect how officers make decisions and prioritise tasks in digital investigations. While digital workflows move earlier in the investigative pipeline, officers remain responsible for evidential integrity while often lacking visibility in terms of how data is stored, transferred, preserved, or processed behind the scenes. On top of this, participants also described how evidence can be lost due to short storage periods. Inconsistent standards across forces, shrinking retention windows, end-to-end encryption, and zero-knowledge storage models mean that certain forms of data may no longer be recoverable even with lawful authority [50]. This can also paradoxically mean that officers feel less in control and more dependent on technical systems they do not fully understand. As digital investigations grow more complex, officers may increasingly offload cognitive effort [51] onto algorithmic systems to manage uncertainty [52].

Regulatory reforms further influence how DE enters the justice pipeline. Proactive moderation under the Online Safety Act 2023 means that automated detection, removal, and algorithmic flagging increasingly determine which material is preserved, reported, or deleted before investigators ever see it. Regulatory compliance therefore shapes what digital material becomes available to investigators in the first place, reinforcing the infrastructural nature of contemporary digital investigations. In response, participants emphasised the need for end-to-end DE processes, interoperable systems, and consistent national standards across forces. This aligns with recent UK government initiatives [53], which acknowledge that without reliable evidence pipelines, advanced analytic tools may amplify rather than resolve evidential weaknesses. Without stable and interoperable systems, officers will struggle to manage workload and justify DE in court [54].

Theme three: This theme highlights the human factors involved in evaluating digital forensic outputs and determining how they should inform investigative decisions. Participants emphasised that the interpretation and use of DE are shaped by human judgement,

trust, and perceptions of fairness. Tyler's procedural justice theory [37] provides a useful framework for understanding these dynamics. It emphasises that institutions are seen as legitimate when their processes are experienced as fair, transparent, and respectful. It is then of growing relevance to apply this theory to the context of DE; investigators must justify how such evidence is obtained, analysed, and relied upon in the face of increasingly complex and technologically mediated data. If officers, courts, or the public alike cannot understand or challenge digital tools, trust in DE can be undermined even when technically accurate or legally justified. Our findings further suggest that proportionality assessments are becoming more complex under AI-mediated conditions, building on the work of Thompson and Manning [20]. For example, in cases involving AI-generated CSAM, uncertainty about whether a real child is depicted complicates decisions about whether a full device examination or arrest is needed.

How officers themselves understand and rely on digital systems also affects legitimacy and proportionality. Officers described interpretive challenges involved in assessing the reliability of DE, particularly when evaluating outputs generated by algorithmic investigative systems. Extending previous work on CCTV and mobile phone data, which demonstrates that digital artefacts require active recovery, interpretation, and narrative framing [3,55], similar interpretive dynamics apply to AI-enabled systems. Our findings suggest that algorithmic outputs can sometimes be treated as conveying strong evidential certainty. These systems require skilled human evaluation and decision-making to critically assess outputs [56]. Prior work similarly emphasises that trust in automation and technological systems depends on transparency, procedural fairness, and accountability [56,57] and clear communication of their limitations and errors [52,58]. When uncertainty is obscured and outputs appear definitive, over-reliance becomes more likely. When such outputs are mis-treated as authoritative, this risks misidentifications, narrows lines of enquiry, and presents overconfident digital "matches" in court, which can further undermine public confidence. These findings highlight the importance of training, feedback, and clear communication in supporting trust, as we will further expound in the next theme.

These concerns reflect broader efforts to strengthen governance around AI and DE in UK policing. Despite increasing deployment of AI-enabled surveillance tools and scholarly concerns that AI and algorithmic tools in policing should not operate in isolation from law [58], the UK lacks a dedicated legislative framework governing technologies such as LFR [30]. Initiatives such as the NPCC AI Ethics Covenant and collaboration with the Forensic Science Regulator seek to ensure AI systems are lawful, proportionate, and transparent [53]. These frameworks recognise that the credibility of DE is supported by ethical governance, scientific validation, and public accountability.

The implications of trust extend beyond officers themselves. In cases where the authenticity of digital material is disputed, victims may fear being dismissed or not being believed [49,59]. While this theme highlights that certain digital outputs may be treated as authoritative, even when their limitations are not fully understood, Theme One also shows that DE is becoming more complex and increasingly contested. Prior research suggests this can create two opposing risks in court: over-trusting technological outputs when they appear objective [17,52,58], or becoming overly sceptical when authenticity is challenged [50]. Recent experimental evidence further indicates that reliance on AI guidance can subtly shape human judgement [60]. This could have potential implications for how juries and other legal decision-makers assess DE.

These findings can also be situated within wider debates in forensic science regarding validity and reliability. The increasing reliance on digital tools and AI assisted systems raises questions consistent with broader critiques of forensic evidence, particularly concerning the need for empirical validation, transparency, and known error rates. While

traditional forensic disciplines have undergone significant scrutiny and standardisation, digital forensics remains comparatively underdeveloped in this regard [12]. Strengthening alignment with forensic science standards, through validation studies, accreditation, and independent testing, will be essential to ensure that DE can meet the same evidential threshold as other forensic domains.

Theme Four: Across interviews, participants described gaps in skills and confidence in the current (and ongoing) use of DE. As investigations become more digital-heavy and technologically complex, participants reported a growing gap between access to digital tools, what digital tools can produce, and what they feel able to interpret in practice. In particular, findings show difficulties officers face in deciphering algorithmic outputs, which are sometimes interpreted as conveying high levels of evidential certainty. Officers therefore need to understand that match decisions are based on similarity scores compared against configurable thresholds, and that false match rates depend on factors such as threshold settings, database size, and image quality [39]. Interpreting operational thresholds, error rates, model limitations, and classification errors has become more crucial than ever in the context of expanding AI and algorithmic use within policing [42,54,56]. Algorithmic outputs should be treated as investigative leads that needs to be critically interpreted by knowledgeable officers [56,61]. Without such competence, officers may either over-rely on algorithmic outputs or dismiss them prematurely.

Officers must also be able to explain complex digital material, such as movement data, platform records, and metadata, clearly and accurately to suspects, victims, juries, and judges. As AI-generated evidence becomes more common, there is a growing need for clear best-practice guidance on how authenticity, uncertainty, and probabilistic reasoning should be explained in court and beyond. Importantly, participants also urged that OSINT training should not be seen as a niche or specialist skill, but as a core competence that all officers need to verify information, assess reliability, and act proportionately. Unlike traditional digital investigations which takes place within formal police systems, OSINT involves gathering information from open online platforms such as social media and websites [10,62]. However, training alone cannot resolve these pressures.

Ongoing national digital reform initiatives [53] emphasise AI deployment, data interoperability, and digital maturity. The College of Policing and NPCC are moving towards building digital reasoning skills, strengthening professional confidence in digital capabilities, including leveraging digital tools for modern crime-solving. Some of such are AI-assisted tools that may help mitigate cognitive overload [54]. While such initiatives show important progress, participants' accounts in this study suggest that current training remains inconsistent across forces and also insufficient in meeting the demands placed on frontline officers. At the same time, practitioners have raised concerns about "snake oil", where AI-labelled systems are marketed as claiming to improve efficiency without proper validation, reliability testing, or transparency [30]. Responsible adoption of AI tools therefore requires critical evaluation skills within the workforce.

5. Limitations

Several limitations of this study should be acknowledged. One drawback is that participants were drawn from policing contexts in England and Wales, where investigative practices are shaped by specific legal frameworks, organisational structures, and accreditation regimes. As a result, findings may not apply directly to other jurisdictions beyond England and Wales. Another limitation is that only two participants identified as female, even if this is indicative of a larger disparity in the field of digital forensics [63]. The predominantly male sample may have influenced how certain issues were articulated and may have limited the range of viewpoints captured in the study. Additionally, participants

who took part in this study may have had greater interest in digital investigations more broadly, whereby the perspectives of less digitally engaged officers may be underrepresented. Finally, although participants discussed challenges related to AI, this study was not intended to expressly examine how AI tools are used in investigations. Future research could explore how officers actually interact with AI, algorithmic systems, and synthetic media in operational contexts.

6. Conclusions

This study suggests, at least in the context of policing in England and Wales, that DE remains an evolving field of practice. Although digital artefacts are now central to investigations, they are not yet consistently understood, interpreted, nor applied. Studying how police investigators interpret DE is essential for understanding how human judgement shapes the way digital traces are turned into meaningful accounts of events and criminal activity. Generative systems such as deepfakes, AI-generated CSAM, and voice clones, as well as model-generated evidential inferences are expanding what counts as DE. This not only introduces new criminal offences to policing, but it is reshaping how officers think, reason, and make decisions about DE. While all forms of evidence have always been open to manipulation, generative AI can now produce convincing digital content that has no real-world origin. This increases uncertainty about the origins of such material and who can be linked to it. DE therefore demands stronger verification and more contextual interpretation. Investigators must determine not only whether material is authentic, but what kind of artefact it represents. This categorisation matters for charging, harm assessment, sentencing, and victim identification. Further, this reshapes investigative interviewing strategies, where focus must shift toward intent, knowledge, and control.

Policing is becoming increasingly digitalised in its everyday operations, as DE is captured, transferred, and stored within complex technological ecosystems, without current sufficient training. Where officers lack confidence or understanding, it affects how they assess digital artefacts and explain it in court. One of the consequences of low digital and systems literacy is that officers may feel dependent on systems they do not understand.

Prior research showed that policing did not always recognise or consistently pursue DE [19,20]. Our findings indicate that these challenges now occur within a more complex landscape involving AI and algorithmic systems, as well as reduced data availability. As digitally mediated surveillance practices expand, including the integration of LFR into drone-based surveillance systems, what is perceived as intrusive or mistrusted risk eroding the very cooperation on which these investigations depend. Trust also depends on clear and consistent end-to-end standards and on officers being able to explain their decisions carefully and fairly to courts and victims alike, without dismissing harm.

Across the four themes, participants emphasised the interpretive work that investigators must do to make sense of digital artefacts within the wider context of investigations, often under conditions of increasing cognitive demand and uncertainty. Findings show that the future of digital forensic investigations will depend in part on investigators' ability to interpret digital artefacts and algorithmic outputs, which provides several directions for future research to continuously advance policing with developing technology within criminality. To cater to this, further research and developments should be made to provide consistency throughout forces on identifying and interpreting DE to provide authenticity, attribution, and evidential value to case work. To help support the consistency required within policing, further exploration of DE training is required to support policing staff when handling cyber-enabled and cyber-dependent crimes. This could be treated as an annual training resource to ensure police officers are aware of core concepts of DE, under-

stand technological implications, how to interpret such data, and are better positioned to handle the increasing digitalisation of criminal investigations.

To move beyond what one participant eloquently describes as the “Enlightenment phase” of digital policing, several practical recommendations emerged based on findings in this study. First, digital literacy must be treated as a priority in policing, including OSINT capabilities. DE training should be standardised across forces to improve consistency in how digital artefacts are identified and interpreted in investigations, and to reduce over-reliance on systems that officers may not fully understand. Second, clear operational guidance should be developed to support officers in distinguishing, documenting, and evidentially categorising AI generated, manipulated, and hybrid digital material. Finally, the validation, independent testing, and transparency reporting of error rates in digital forensic tools should be strengthened to address inconsistencies in outputs and support evidential reliability in both investigations and court proceedings.

Author Contributions: All authors contributed to the development of the interview protocol. M.N. conducted the interviews and analysed the data, with R.M. overseeing coding of data. M.N. wrote the manuscript and conceptualised all figures and tables. C.J.D. and R.M. edited the manuscript, and all authors (C.J.D., R.M.) reviewed the final manuscript. CRediT authorship contribution statement—M.N.: Conceptualisation, Data curation, Formal analysis, Investigation, Methodology, Project administration, Writing—original draft, Writing—review & editing. R.M.: Formal analysis, Writing—original draft, Writing—review & editing. C.J.D.: Writing—review & editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki and approved by the Ethics Committee of the University of Westminster (protocol code ETH2425-0936).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Study materials and interview protocol are available via the Open Science Framework at https://osf.io/eapsh/overview?view_only=0399cd7114f0464783b593c02d54e4d8 (accessed on 7 February 2026).

Acknowledgments: The authors thank the University of Westminster’s Research Centre Residential Writing Retreat for providing the necessary space and dedicated writing time to complete this project. We would like to thank Tina Cartwright (not named author) for her guidance and expertise in conducting a reflexive thematic analysis. We would also like to thank the police officers who generously contributed their time and insights to this research.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Reflexive Statement

The first author has research expertise in forensic psychology, with particular interests in digital evidence, human–technology interaction, and investigative interviewing. This background informed the study’s research questions and interpretation of participants’ accounts. Themes were developed through an iterative approach that acknowledged active engagement interpreting the data, in keeping with reflexive thematic analysis [64]. Throughout the analysis, the author reflected on how prior knowledge and assumptions might shape interpretation. To further reduce potential disciplinary blind spots, the research team included co-authors with expertise in digital forensics and policing practice, where interpretations were discussed regularly as a team.

References

1. Wilson-Kovacs, D.; Helm, R.; Grown, B.; Redfern, L. Digital evidence in defence practice: Prevalence, challenges and expertise. *Int. J. Evid. Proof* **2023**, *27*, 235–253. [\[CrossRef\]](#)
2. Guttman, B.; White, D.R.; Walraven, T. *Digital Evidence Preservation: Considerations for Evidence Handlers*; NIST IR 8387; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2022.
3. Brookman, F.; Jones, H. Capturing killers: The construction of CCTV evidence during homicide investigations. *Polic. Soc.* **2022**, *32*, 125–144. [\[CrossRef\]](#)
4. Jones, H.; Brookman, F. Risky calls: Understanding the challenges and risks of using mobile phone data during homicide investigations. *Polic. Soc.* **2024**, *34*, 1091–1107. [\[CrossRef\]](#)
5. Ng, M.; Medhurst, R.; Dando, C.J.; Bull, R. “A Ronin Without a Master”: Exploring police perspectives on digital evidence in England and Wales. *Behav. Sci.* **2025**, *15*, 1416. [\[CrossRef\]](#)
6. Sandham, A.; Ormerod, T.; Dando, C.; Bull, R.; Jackson, M.; Goulding, J. Scent trails: Countering terrorism through informed surveillance. In *International Conference on Engineering Psychology and Cognitive Ergonomics*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 452–460.
7. Wilson-Kovacs, D. Digital media investigators: Challenges and opportunities in the use of digital forensics in police investigations in England and Wales. *Polic. Int. J.* **2021**, *44*, 669–682. [\[CrossRef\]](#)
8. Heath, H.; MacDermott, Á.; Akinbi, A. Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data? *Forensic Sci. Int. Digit. Investig.* **2023**, *46*, 301585. [\[CrossRef\]](#)
9. Horsman, G. Can we continue to effectively police digital crime? *Sci. Justice* **2017**, *57*, 448–454. [\[CrossRef\]](#)
10. Quick, D.; Choo, K.K.R. Digital forensic intelligence: Data subsets and OSINT. *Future Gener. Comput. Syst.* **2018**, *78*, 558–567. [\[CrossRef\]](#)
11. Her Majesty’s Inspectorate of Constabulary and Fire & Rescue Services. *Digital Forensics: An Inspection into How Well the Police and Other Agencies Use Digital Forensics in Their Investigations*; His Majesty’s Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS): London, UK, 2022.
12. Ng, M.; James, J.; Bull, R. “What you say in the lab, stays in the lab”: A reflexive thematic analysis of digital forensic investigations in the UK. *Forensic Sci. Int. Digit. Investig.* **2024**, *51*, 301839.
13. Casey, E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*; Academic Press: Cambridge, MA, USA, 2011.
14. National Police Chiefs’ Council (NPCC). *Artificial Intelligence (AI) Playbook for Policing*; NPCC AI Portfolio: London, UK, 2025.
15. Conway, M. Determining the role of the internet in violent extremism and terrorism. *Stud. Confl. Terror.* **2017**, *40*, 77–98. [\[CrossRef\]](#)
16. Jones, H.; Brookman, F.; Williams, R.; Fraser, J. We need to talk about dialogue: Collaborative sensemaking in homicide investigations. *Police J.* **2021**, *94*, 572–589. [\[CrossRef\]](#)
17. Wilson-Kovacs, D.; Jones, H.; Brookman, F. The use of digital evidence in homicide investigations. In *Routledge Handbook of Homicide Investigation*; Routledge: Abingdon, UK, 2024.
18. Hadlington, L.; Lumsden, K.; Black, A.; Ferra, F. Police officers’ perceptions of cybercrime. *Policing* **2021**, *15*, 34–43. [\[CrossRef\]](#)
19. Goodison, S.E.; Davis, R.C.; Jackson, B.A. *Digital Evidence and the US Criminal Justice System*; RAND Corporation: Santa Monica, CA, USA, 2015.
20. Thompson, P.; Manning, M. Missed opportunities in digital investigations. In *Cybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability, London, January 2021*; Springer: Cham, Switzerland, 2021; pp. 101–122.
21. Horsman, G. Interpreting digital traces: 8 foundational pillars to support the formation of opinion in digital forensics. *Sci. Justice* **2024**, *64*, 38–42. [\[CrossRef\]](#)
22. Morgan, R.M.; Levin, E.; Biriotti, M. Interpretation of forensic text-based communications. *Forensic Sci. Int. Synerg.* **2026**, *12*, 100667. [\[CrossRef\]](#)
23. Dando, C.J.; Ormerod, T.C. Decision making in serious crime investigations. *Hum. Factors* **2017**, *59*, 1188–1203. [\[CrossRef\]](#)
24. Braun, V.; Clarke, V. To saturate or not to saturate? *Qual. Res. Sport Exerc. Health* **2021**, *13*, 201–216. [\[CrossRef\]](#)
25. Braun, V.; Clarke, V. Reflecting on reflexive thematic analysis. *Qual. Res. Sport Exerc. Health* **2019**, *11*, 589–597. [\[CrossRef\]](#)
26. Braun, V.; Clarke, V. One size fits all? *Qual. Res. Psychol.* **2021**, *18*, 328–352. [\[CrossRef\]](#)
27. Braun, V.; Clarke, V. Using thematic analysis in psychology. *Qual. Res. Psychol.* **2006**, *3*, 77–101. [\[CrossRef\]](#)
28. Finn, R.L.; Wright, D. Unmanned aircraft systems. *Comput. Law Secur. Rev.* **2012**, *28*, 184–194. [\[CrossRef\]](#)
29. Levine, M. *Identity, Surveillance and Privacy*; SPRITE+/N8PRP event; SPRITE+: Manchester, UK; N8PRP: Leeds, UK, 2025.
30. Brown, T.B.; Mann, B.; Ryder, N.; Subbiah, M.; Kaplan, J.D.; Dhariwal, P.; Neelakantan, A.; Shyam, P.; Sastry, G.; Askell, A.; et al. Language models are few-shot learners. *arXiv* **2020**, arXiv:2005.14165. [\[CrossRef\]](#)
31. Bommasani, R.; Hudson, D.A.; Adeli, E.; Altman, R.; Arora, S.; von Arx, S.; Bernstein, M.S.; Bohg, J.; Bosselut, A.; Brunskill, E.; et al. On the opportunities and risks of foundation models. *arXiv* **2021**, arXiv:2108.07258. [\[CrossRef\]](#)

32. Rombach, R.; Blattmann, A.; Lorenz, D.; Esser, P.; Ommer, B. High-resolution image synthesis with latent diffusion models. *arXiv* **2022**, arXiv:2112.10752. [CrossRef]
33. Google DeepMind. Gemini: A Family of Highly Capable Multimodal Models. *arXiv* **2023**, arXiv:2312.11805.
34. OpenAI. GPT-4 technical report. *arXiv* **2023**, arXiv:2303.08774.
35. Burton, J.; Janjeva, A.; Moseley, S.; Alice. *AI and Serious Online Crime*; Alan Turing Institute: London, UK, 2025.
36. Belshaw, S.; Nodeland, B. Digital evidence experts in policing. *Secur. J.* **2022**, *35*, 248–262. [CrossRef]
37. Tyler, T.R. *Why People Obey the Law*; Yale University Press: New Haven, CT, USA, 1990.
38. Tyler, T.R. Psychological perspectives on legitimacy and legitimation. *Annu. Rev. Psychol.* **2006**, *57*, 375–400. [CrossRef]
39. Grother, P.; Ngan, M.; Hanaoka, K. *Face Recognition Vendor Test*; NIST: Gaithersburg, MD, USA, 2019.
40. Horsman, G. Tool testing and reliability issues. *Digit. Investig.* **2019**, *28*, 163–175. [CrossRef]
41. Carrier, B.D.; Spafford, E.H. Digital investigation techniques. *Digit. Investig.* **2006**, *3*, 121–130. [CrossRef]
42. Gillespie, A.A. *Child Pornography: Law and Policy*; Routledge: Abingdon, UK, 2012.
43. Ormerod, D.C. Indecent pseudo-photographs. *Crim. Law Rev.* **2004**, 1039–1041.
44. Surrey Police & Sussex Police. *Deepfake Technology Policy (1241/2024)*; Surrey Police: Guildford, UK; Sussex Police: Lewes, UK, 2024. Available online: <https://www.sussex.police.uk/SysSiteAssets/foi-media/sussex/policies/deepfake-technology-policy-surrey-and-sussex-1241.pdf> (accessed on 7 February 2026).
45. UK Parliament. *Online Safety Act 2023*; The Stationery Office: London, UK, 2023.
46. EU. *Regulation (EU) 2022/2065 (Digital Services Act)*; EU: Brussel, Belgium, 2024.
47. Department for Science, Innovation and Technology; Kendall, L.; Phillips, J. New Law to Tackle AI Child Abuse Images at Source as Reports More Than Double. *GOV.UK*, 12 November 2025. Available online: <https://www.gov.uk/government/news/new-law-to-tackle-ai-child-abuse-images-at-source-as-reports-more-than-double> (accessed on 7 February 2026).
48. Science & Technology in Policing. Insights from the Generative AI Academic Advisory Group: January 2025. 2025. Available online: <https://science.police.uk/delivery/resources/insights-from-the-generative-ai-academic-advisory-group-january-2025/> (accessed on 7 February 2026).
49. Chesney, B.; Citron, D. Deep fakes. *Calif. Law Rev.* **2019**, *107*, 1753.
50. Bellovin, S.M.; Blaze, M.; Clark, S.; Landau, S. Going Bright: Wiretapping Without Weakening Communications Infrastructure. *IEEE Secur. Priv.* **2014**, *11*, 62–72. [CrossRef]
51. Dror, I.; Harnad, S. *Offloading Cognition*; John Benjamins: Philadelphia, PA, USA, 2008.
52. Dzindolet, M.T.; Peterson, S.A.; Pomranky, R.A.; Pierce, L.G.; Beck, H.P. The role of trust in automation reliance. *Int. J. Hum.-Comput. Stud.* **2003**, *58*, 697–718. [CrossRef]
53. National Police Chiefs' Council. *NPCC Innovation & Digital Summit*; National Police Chiefs' Council: Liverpool, UK, 2025.
54. Fussey, P.; Murray, D. *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*; University of Essex: Colchester, UK, 2019. Available online: <https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf> (accessed on 7 February 2026).
55. Jones, H.; Brookman, F. Backstage at the barristers' case conference: A dramaturgical analysis. *J. Contemp. Ethnogr.* **2023**, *53*, 3–30. [CrossRef]
56. Oswald, M. Trustworthy AI in policing. *Eur. J. Law Technol.* **2022**, *13*.
57. Jackson, J.; Bradford, B.; Hough, M.; Myhill, A.; Quinton, P.; Tyler, T.R. Why do People Comply with the Law? Legitimacy and the Influence of Legal Institutions. *Br. J. Criminol.* **2012**, *52*, 1051–1071. [CrossRef]
58. Lee, J.D.; See, K.A. Trust in automation. *Hum. Factors* **2004**, *46*, 50–80. [CrossRef]
59. Vaccari, C.; Chadwick, A. Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. *Soc. Media Soc.* **2020**, *6*, 2056305120903408. [CrossRef]
60. Pearson, J.; Dror, I.E.; Jayes, E.; Whordley, G.-R.; Mason, G.; Nightingale, S. Examining human reliance on artificial intelligence in decision making. *Sci. Rep.* **2026**, *16*, 5345. [CrossRef]
61. El Fadel, N. Facial recognition algorithms. *J. Imaging* **2025**, *11*, 58. [CrossRef]
62. Pastor-Galindo, J.; Nespoli, P.; Mármol, F.G.; Pérez, G.M. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access* **2020**, *8*, 10282–10304. [CrossRef]
63. Wagstaff, I.R.; LaPorte, G. The importance of diversity and inclusion in the forensic sciences. *NIJ J.* **2018**, *279*, 81–91.
64. Braun, V.; Clarke, V.; Hayfield, N.; Davey, L.; Jenkinson, E. Doing reflexive thematic analysis. In *Supporting Research in Counselling and Psychotherapy: Qualitative, Quantitative, and Mixed Methods Research*; Springer International Publishing: Cham, Switzerland, 2023; pp. 19–38.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.