Forensic Science International: Digital Investigation 56 (2026) 302058

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

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

DFRWS EU 2026 - Selected Papers from the 13th Annual Digital Forensics Research Conference Europe

Ctrl+Alt+Deceit: Policing the Deepfake Dilemma

Áine MacDermott

School of Computer Science and Mathematics, Liverpool John Moores University, UK

ARTICLE INFO

Keywords:
Digital forensics
Practitioner survey
Challenges
Deepfake forensics
Recommendations

ABSTRACT

In a digital world where "truth" can be rewritten with a few lines of code, *Ctrl + Alt + Deceit* has become the new normal for forensic practitioners. The rapid growth of deepfake technologies presents a mounting challenge for digital forensics, threatening the integrity and reliability of multimedia evidence. This paper presents findings from a practitioner-focused survey designed to assess the real-world impact of synthetic media on forensic workflows. The study explores the prevalence of deepfake-related cases, regional trends in AI-generated media, and the operational readiness of digital forensic units (DFUs) to respond to these emerging threats. Despite increasing interest in detection technologies, the results reveal a substantial gap between technical capabilities and practical deployment, with many DFUs operating without formal guidance, policy structures, or legislative backing. The paper concludes with a set of best practice recommendations tailored to the unique demands of deepfake forensics, offering insights to support both practitioners and researchers in developing robust, informed approaches to multimedia evidence in the era of synthetic media.

1. Introduction and background

The rapid rise of deepfake technology is reshaping how authenticity and trust are established in digital evidence. Deepfake forensics - the application of digital forensic and analytical techniques to detect and interpret synthetic media - combines elements of computer science, machine learning, and multimedia analysis to determine whether audio, video, or imagery has been artificially generated or altered.

This paper presents a practitioner-focused contribution to DFRWS EU by addressing one of the most rapidly evolving challenges in digital forensics: the proliferation of deepfake media across image, audio, and video formats. As generative models become more sophisticated and accessible, their impact on evidential integrity, victim identification, and trust in digital content are profound.

To explore this evolving landscape, a targeted survey was conducted among professionals from law enforcement, academia, consultancy, and research to assess how deepfakes are perceived and encountered in practice. The study offers empirical insight into detection capabilities, operational readiness, and organisational guidance. Findings aim to inform both policy and practice, while fostering interdisciplinary collaboration on robust approaches to synthetic media forensics.

While research into the implications of deepfake media within digital forensics and cybersecurity is growing - particularly in relation to misinformation, identity fraud, and evidentiary integrity – a notable gap remains in understanding how practitioners engage with detection tools and technologies. While usability studies have examined aspects such as interface design and data presentation in forensic tools such as Silva et al. (2022) and Qureshi et al. (2024), few have focused specifically on the operational value and reliability of deepfake detection technologies from the perspective of investigators (MacDermott, 2025a).

The practitioner survey was designed to address the following research questions:

RQ1: How have deepfakes impacted digital forensic investigations and cybersecurity workflows, and what challenges do practitioners encounter when detecting and analysing this content?

RQ2: Do practitioners perceive an increase in deepfake and synthetic media cases?

RQ3: What gaps exist in current tools, training, and methodologies for deepfake detection and forensic analysis, and how can these be addressed to improve investigative best practices?

By examining how practitioners navigate deepfake-related investigations, this work aims to guide future research, tool development, and policy frameworks. The findings also support the creation of more resilient workflows, reduce investigative overhead, and enhance the evidential reliability of multimedia content in forensic contexts. The key contributions of this study are as follows.

- It is the first comprehensive survey to examine practitioner experiences with deepfake media across multiple sectors, including law enforcement, academia, consultancy, and research.

E-mail address: a.m.macdermott@ljmu.ac.uk.

https://doi.org/10.1016/j.fsidi.2026.302058

- It provides empirical data on the perceived effectiveness of AI-driven detection tools and highlights practitioner concerns around legislation, workflows, and tool reliability.
- It identifies critical gaps in institutional guidance, training, and preparedness, offering a foundation for future collaboration between researchers, developers, and policymakers.
- A dataset containing the responses to the survey, allowing researchers and the academic community to further analyse.

The structure of this paper is as follows: Section 2 highlights Related Work that underpins our approach. Section 3 outlines our Research Aims and Objectives. Section 4 details the Methodology, followed by presentation of Results in Section 5. Section 6 offers a Discussion and Evaluation of our findings. Section 7 presents our Conclusions and Recommendations.

2. Related Work

Although deepfake media has garnered growing attention in digital forensics and cybersecurity discourse, there remains a notable gap in targeted research addressing the specific challenges deepfakes pose to forensic investigations - particularly in terms of how they can undermine or complicate evidentiary processes.

Several foundational studies have examined the evolution of digital forensic research and its methodological challenges, e.g., Garfinkel (2010) analysed and mapped key forensic challenges and research directions for the following decade, while Lyle et al. (2022) critically assessed the scientific foundations of digital forensic methods, examining their reliability, limitations, and legal applicability in investigative contexts. Similarly, Breitinger et al. (2024) offered a ten-year retrospective of DFRWS EU, identifying persistent issues such as tool validation, reproducibility, and the integration of emerging technologies, alongside recommendations for future research. Despite these contributions, few studies have systematically examined how practitioners evaluate the functionality and operational impact of deepfake detection tools in real-world investigations.

Sanchez et al. (2019) designed and distributed a survey to digital forensic practitioners working on Child Sexual Abuse Material (CSAM) investigations. It aimed to understand how these professionals use and evaluate forensic tools, especially those incorporating AI and filtering technologies. Responses were analysed to identify gaps in tool usage, training, and workflow efficiency, informing future development in forensic technologies. More recently, the *DFPulse: The 2024 Digital Forensic Practitioner Survey* (Hargreaves et al., 2024) collected 122 responses across disciplines to understand practitioner environments, investigative techniques, and challenges. It also examined how academic research is accessed and valued, helping to shape future research priorities.

Interestingly, Interpol (2024) and the U.S. Department of Homeland Security (2023) offer practical, real-world perspectives on the risks and mitigation strategies associated with deepfakes, with findings that can be aligned to our study. Interpol (2024) provides background on deepfakes and other synthetic media types, detailing a range of criminal uses, challenges for law enforcement, and broader societal implications. Similarly, the U.S. Department of Homeland Security (2023) presents scenarios illustrating deepfake threats across commerce, society, and national security, emphasising that no single solution exists; instead, effective mitigation requires a combination of technical innovation, education, and regulation.

These insights highlight the growing need to collect statistics on cases or incidents involving deepfake media, as well as the prevalence of AI-generated forgeries (such as fabricated images, audio, and video) across different regions and sectors. Building on the methodologies from prior surveys, this research adopts a practitioner-focused approach to ensure relevance and applicability to real-world investigative contexts. Previous studies have shown the value of engaging directly with professionals to uncover operational challenges, tool limitations, and sector-specific vulnerabilities. By following this approach, our study seeks not only to document practitioner experiences with deepfake media but also to generate actionable insights grounded in empirical data. This evidence-based perspective supports the development of practical solutions and informed policy recommendations to enhance digital forensic capabilities against emerging threats.

3. Research Aims and Objectives

The overarching aim of this study is to investigate digital forensic practitioners' experiences, perceptions, and technical understanding of deepfakes and other manipulated media, to.

- Identify current challenges and gaps in detection and analysis methods.
- Inform the creation of best practices and robust methodologies for handling fabricated digital content within forensic and cybersecurity contexts.
- Generate useable statistics and produce an anonymised dataset, enabling researchers and the academic community to conduct further analysis and advance the field of synthetic media forensics.

To achieve this aim and address the research questions outlined in Chapter 1, we established the following objectives.

- The survey will be conducted over a 6 month period via JISC Online Surveys.
- Responses will be collected from at least 50 practitioners across law enforcement, academia, consultancy, and industry to measure awareness of deepfake technologies, detection techniques, and associated forensic challenges.
- Quantitative survey data will be analysed to generate useable descriptive and inferential statistics (e.g., frequency, cross-tabulations) that provide insight into practitioner awareness, operational readiness, and tool adoption.
- The survey will include thematic analysis of open-ended responses to identify major themes that reveal gaps in current detection tools, training provision, and guidance for synthetic media.
- We will publish a clean, anonymised dataset in an open-access repository to support transparency, reproducibility, and future research.
- Practitioner-focused recommendations will be produced, informed by empirical survey findings and disseminated through professional channels.

4. Methodology

The survey consisted of three pages and was administered via JISC Online Surveys under LJMU Research Ethics Committee Reference Number 25/CMP/004. A copy of the dataset is available for download (Mac Dermott, 2025b), with selected items of interest included in the Appendix.

The survey began by obtaining participant consent, followed by a brief demographic section containing four questions. On the second page, the consent process was reiterated, emphasising that participation was entirely voluntary and that respondents could withdraw at any time without consequence. The third page presented a series of technical questions designed to explore the impact and implications of deepfakes and other fabricated media within digital forensic investigations and the broader cyber domain. The survey combined Likert-scale questions and open-ended items, designed to capture both quantitative and qualitative insights. These questions aimed to assess participants' understanding of deepfake and manipulated media, detection techniques, and the forensic challenges associated with identifying and analysing digitally manipulated content.

4.1. Data collection

The survey collected data on participants' experiences and perceptions regarding deepfakes and their impact on digital forensics and cybersecurity. It explored whether respondents viewed the rise of deepfakes as an increasing challenge, and whether they had encountered deepfakes or other forms of manipulated media in their professional roles. Participants were also asked to estimate the number of cases or incidents they had handled that required analysis of deepfake content, and to reflect on the difficulty of verifying its authenticity.

Overall, the survey was designed to capture practitioner insights into the evolving challenges posed by deepfakes, with the goal of informing and shaping future investigative best practices. By gathering real-world experiences and expert perspectives, it sought to identify current gaps in detection and analysis methods, understand the practical impact of deepfake media on forensic workflows, and support the development of more robust methodologies for handling manipulated digital content in professional settings.

4.2. Promotion and recruitment

The survey recruitment was promoted through multiple channels, including a Poster Presentation and Lightning Talk at DFRWS EU 2025, a Women in Forensic Computing (WinFC) 2025 presentation, and the WinFC mailing list. Additional advertisements were shared via the Forensic Focus website and its social media platforms, as well as on LinkedIn, X, and Bluesky. A snowball sampling approach was also employed, encouraging recipients to share the survey link with colleagues. The survey was open from March to October 2024 and received 59 responses. Participation was fully anonymous, and no identifying information was collected.

4.3. Data analysis

Data was analysed in JISC and exported as a CSV for a tabular breakdown. The survey primarily focused on qualitative analysis through free-text responses, allowing participants to share detailed insights and experiences related to deepfakes in their professional roles. However, to contextualise these narratives, we also included demographic analysis, presenting participant characteristics (such as gender, role, country of residence, and qualifications) as percentages. This helped frame the qualitative data within a broader understanding of the respondents.

4.4. Presentation of results

The results of the survey are both visualised and explained to enhance clarity and accessibility. The analysis makes use of tables and figures, with a particular emphasis on bar charts, which effectively represent the distribution of responses across different categories. These visual tools help to highlight key trends and variations in participant feedback, making it easier to interpret the data alongside the qualitative insights. Data has been cleaned where required, e.g. an option that has no response, or a response irrelevant to the question.

5. Results

The survey included demographic questions focusing on gender, current role, country, and education. The overall profile of the participants is summarised in Table 1, with details discussed in the upcoming subsections (Figs. 1-6).

Table 1
Demographic overview $n = 59$.

Gender	n	Percentage
Female	14	24 %
Male	40	68 %
Prefer not to say	5	8 %
Role	**n**	**Percentage**
Academic/Lecturer	17	29 %
Student	2	3 %
Researcher	6	10 %
Law enforcement/gov. Agency	13	22 %
Cyber consultant	11	19 %
Digital forensic consultant	4	7 %
Other	6	10 %
Country	**n**	**Percentage**
Ireland	2	3 %
United Kingdom	46	78 %
United States	1	2 %
Germany	1	2 %
Netherlands	1	2 %
Canada	1	2 %
Switzerland	1	2 %
International/Cross Border	5	8 %
Prefer not to say	1	2 %
Education	**n**	**Percentage**
Secondary School/High School	3	5 %
College	3	5 %
BSc or equivalent	17	29 %
MSc or equivalent	16	27 %
PhD	19	32 %
Continuous Professional Development (CPD)	1	2 %

5.1. Gender and country

The majority of participants identified as male ($n = 40$, 68 %), while 24 % ($n = 14$) identified as female, and 8 % ($n = 5$) chose not to disclose their gender. No participants selected the non-binary and other gender options.

Most respondents were based in the United Kingdom ($n = 46$, 78 %). Other were from International/Cross border ($n = 5$, 8 %), Ireland ($n = 2$, 3 %), and the United States, Germany, the Netherlands, Canada, and Switzerland each had one participant.

5.2. Current role

Participants were asked to specify their current professional role. The largest group identified as Academic/Lecturer ($n = 17$, 29 %), followed by those working in Law enforcement or government agencies ($n = 13$, 22 %) and Cyber consultants ($n = 11$, 19 %). Smaller proportions included Researchers ($n = 6$, 10 %), Digital forensic consultants ($n = 4$, 7 %), and Students ($n = 2$, 3 %). 10 % ($n = 6$) selected Other, reflecting a diverse range of roles within the digital forensics and cybersecurity landscape.

5.3. Education

The participants were also asked to report their highest level of qualification. Out of 59 participants, the majority hold advanced degrees, with 32 % ($n = 19$) having a PhD, and 27 % ($n = 16$) holding an MSc or equivalent. 29 % ($n = 17$) reported a BSc or equivalent. A small number of respondents reported College-level education (5 %, $n = 3$) or Secondary school/High school (5 %, $n = 3$). Only 1 respondent (2 %) indicated Continuous Professional Development (CPD) as their highest qualification.

5.4. Practitioner insights

When asked whether the rise in deepfakes is perceived as an increasing problem for the digital forensics and cybersecurity field, an overwhelming majority of respondents - 90 % ($n = 53$) - answered 'Yes', indicating strong concern across the community. Only 7 % ($n = 4$)

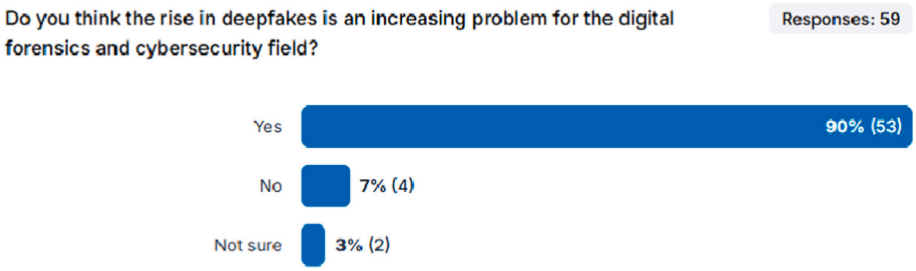

Fig. 1. Increasing problem responses.

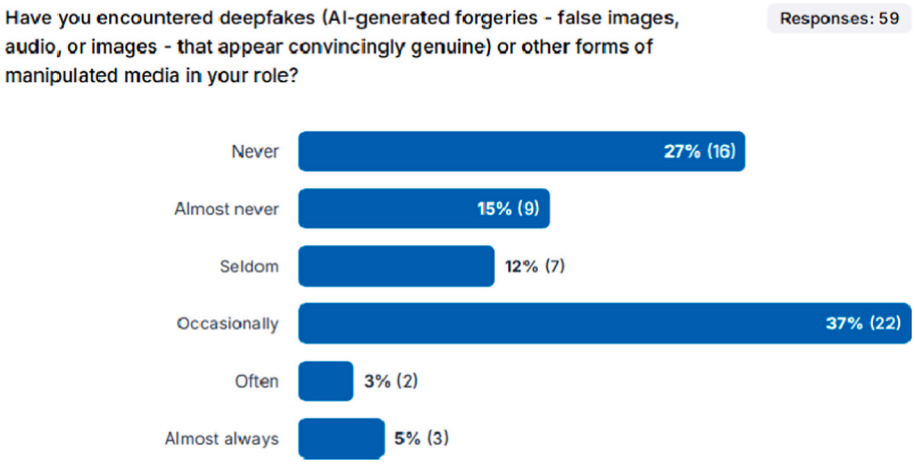

Fig. 2. Deepfake encounters in role.

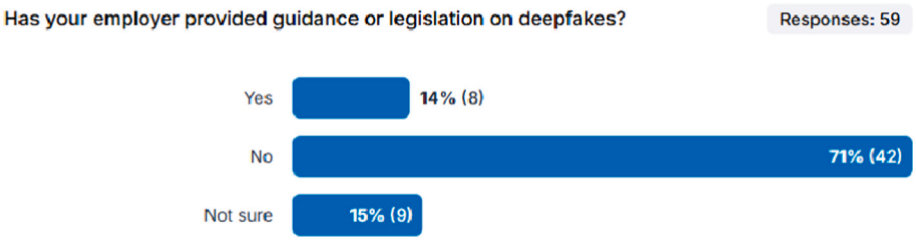

Fig. 3. Employer guidance or legislation.

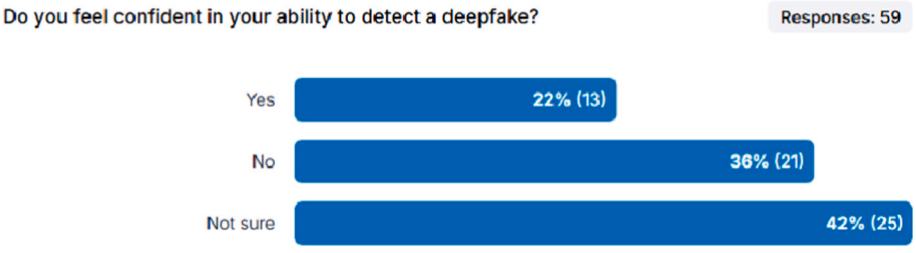

Fig. 4. Confidence in ability to detect a deepfake

responded 'No', and 3 % ($n = 2$) were 'Not sure'.

When asked if they have encountered deepfakes or other forms of manipulated media in their professional roles, the responses indicated a varied but substantial level of exposure. Out of 59 respondents.

- Over a third of respondents (37 %, $n = 22$) indicated that they encounter deepfakes occasionally, suggesting that while such media is not yet a routine aspect of their professional activities, it is becoming increasingly prevalent. A smaller but notable group (5 %, $n = 3$) reported encountering deepfakes almost always, highlighting that for some, these synthetic media are a persistent and regular feature of their work environment. While a smaller amount reported encountering deepfakes seldom (12 %, $n = 7$) or often (3 %, $n = 2$).
- 27 % ($n = 16$) stated they had never encountered deepfakes, and 15 % ($n = 9$) said almost never, indicating that for a significant portion, direct exposure remains limited.

This distribution suggests that while deepfakes are not yet a daily operational concern for most, they are becoming a recurring issue for a

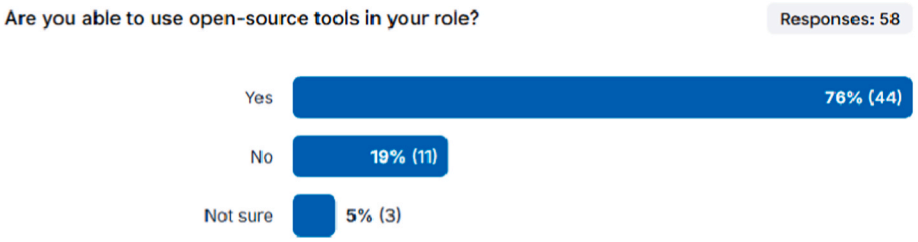

Fig. 5. Ability to use open-source tools in role.

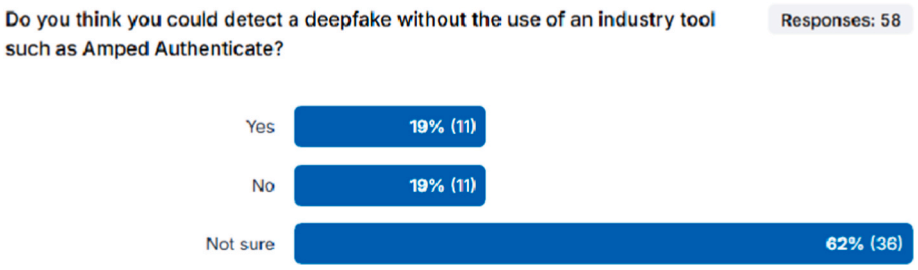

Fig. 6. Ability to detect a deepfake without industry tool.

growing number of practitioners. A follow question, *'If yes please give an example of how deepfakes could be a problem in your job role'* had 35 responses and are summarised in Table 2 (Appendix). The responses revealed several recurring themes concerning the perceived impact of deepfakes in professional settings. Specifically, six key themes emerged.

- **Operational burden and detection difficulties:** Deepfakes are described as time consuming to detect - the increasing quality of deepfakes makes detection more complex and labour-intensive. Also, questions arose about appropriate tools for use and benchmarks, operational burden (especially when case backlogs are present).
- **Criminal exploitation:** Deepfakes are increasingly used in criminal activities such as fraud, money laundering, revenge pornography, and CSAM. Respondents from law enforcement and consultancy roles highlighted their use in blackmail, intimidation, and misinformation campaigns.
- **Media integrity:** Respondents expressed concern over media provenance, especially in forensic and legal contexts. The existence of deepfakes may undermine juror confidence and complicate evidentiary validation.
- **Social engineering and cyber security threats:** Many participants noted deepfakes being used for impersonation, phishing, vishing, and identity fraud that can affect their workplace.
- **Challenges in academia:** Deepfakes are affecting student assessments, with fabricated media being submitted as coursework. This raises concerns about academic integrity, authentication, and the difficulty of verifying multimedia evidence in educational settings.
- **Emerging threats:** Several responses pointed to malvertising and AI-generated misinformation as growing concerns. There is also apprehension about AI-generated research reports, fake credentials, and fabricated internal misconduct evidence, indicating a broadening threat landscape.

5.4.1. *Guidance or legislation*

Respondents were asked whether their employer had issued any formal guidance, or legislation on deepfakes.

71 % ($n = 42$) reported that their employer has not provided any guidance or legislation on deepfakes. Only 14 % ($n = 8$) indicated that such guidance exists, while 15 % ($n = 9$) were unsure. These findings reveal a substantial gap in institutional support for addressing deepfake threats and underscore the need for robust methodologies, targeted training, and comprehensive policy frameworks to strengthen forensic capabilities.

5.4.2. *Confidence in ability*

Participants were asked whether they felt confident in their ability to detect a deepfake, aiming to assess practitioner self-perception of skill and preparedness in identifying synthetic media. The responses show that a majority of the respondents lack confidence in their ability to detect deepfakes.

Out of 59 participants, only 22 % ($n = 13$) felt confident, while 36 % ($n = 21$) said they were not confident, and 42 % ($n = 25$) were unsure. This indicates that nearly four out of five respondents either doubt their detection skills or are uncertain about their capabilities.

A study by Lewis et al. (2023) found that familiarity with deepfakes does not necessarily improve one's ability to detect them. In a controlled experiment involving over 1000 UK participants, only 21.6 % correctly identified a deepfake video from a set of five, even when warned that one of the videos was manipulated. The findings suggest that prior awareness or familiarity with deepfakes does not significantly enhance detection accuracy, highlighting a critical gap between recognition and reliable identification.

5.4.3. *Cases and incidents*

Participants were asked to estimate how many cases or incidents they had been involved in that required the analysis of deepfake media, and to reflect on how easy it was to determine the authenticity of such content. This question aimed to gather practical insights into the frequency of deepfake encounters in investigative work and the challenges associated with verifying synthetic media.

There were 49 respondents, shown in Table 3 (Appendix). Analysis of the responses reveals several key patterns.

- **No experience:** The majority of respondents (28 out of 49) reported having no direct experience with deepfake media in their investigative work. This includes responses such as *"none," "zero."*
- **Some experience:** A smaller group (9 respondents) indicated limited or occasional exposure, e.g. *"minimal," "a few," "1–2 per week,"* or *"10 a year."* These responses suggest that while deepfakes are not yet widespread in daily casework, they are beginning to surface more frequently.
- **Detection difficulty:** 5 respondents specifically commented on the challenges of detecting deepfakes, referencing inconsistent

metadata, visual anomalies, or the need for forensic analysis. This highlights variability in detection success and the limitations of current tools.
- **Observational/contextual insights:** 2 responses provided broader observations about the rise of deepfakes in social media and the increasing sophistication of AI-generated content, suggesting growing awareness even among those not directly investigating such cases.

Overall, the data suggests that, while many practitioners have not yet encountered deepfakes in their casework, there is a growing awareness of the issue and recognition of the challenges associated with detection. Some respondents used the narrative portion of the survey to provide insights into the area, even without specifying a number of cases or incidents.

5.4.4. Effectiveness of current tools

Respondents were asked to share their opinion on how effective current AI-driven detection tools are in identifying deepfake content. Analysis of 51 responses regarding the effectiveness of current AI-driven deepfake detection tools reveals a generally critical and cautious outlook.

- **Not Effective:** The largest group (14 respondents) expressed scepticism about the reliability of current tools, citing issues such as false positives/negatives, underdevelopment, and the delay between detection capabilities and deepfake generation.
- **Effective:** Only 9 respondents considered the tools reasonably effective, by noting effectiveness with older or less sophisticated deepfakes.
- **Somewhat Effective:** 7 respondents described the tools as average or partially effective, often noting variability in performance.
- **Uncertain/No Experience:** 9 respondents indicated they had not used such tools or were unsure of their effectiveness, suggesting limited exposure or institutional access.
- **Mixed/Variable:** 6 responses highlighted that effectiveness depends on the tool, context, or case, reflecting inconsistency across available solutions.

5.4.5. Open-source tools

When asked if they were able to use open-source tools in their role.

A significant number ($n = 44$, 76 %) of respondents reported the ability to use open-source tools in their role, which presents a promising opportunity for integration into forensic software suites or for use in post-imaging analysis workflows. Moreover, there is scope to explore the development of standalone open-source forensic utilities, which could offer flexible, cost-effective solutions while promoting transparency and community-driven innovation. This trend highlights the potential for open-source contributions to help bridge current gaps in tooling and standardisation across the sector.

5.4.6. Detection ability without industry tool

When asked about their ability to detect a deepfake without the aid of industry-standard tools, 62 % ($n = 36$) of respondents reported being *'Not Sure'*, indicating a widespread lack of confidence in manual or unaided detection methods. Only 19 % ($n = 11$) felt confident in their ability to identify deepfakes unaided, while another 19 % ($n = 11$) explicitly stated they could not. This distribution suggests that, despite growing awareness of deepfakes, the skill to reliably detect them without technological support remains limited.

It highlights the critical need for accessible, validated tools and training to support professionals in making accurate assessments that can be validated and verified.

5.4.7. Vulnerable sectors

Participants were asked to identify which industries or sectors they believe are most vulnerable to deepfake-related threats. This question aimed to capture practitioner perspectives on where synthetic media poses the greatest risks, based on their professional experience and observations. Of 51 responses, the most frequently mentioned sectors were.

- Finance (9 mentions) and Banking (5 mentions), were often cited due to risks of fraud, impersonation, and financial manipulation.
- Media (8 mentions) and Politics (6 mentions), reflecting concerns about misinformation, fake news, and reputational harm.
- Government (6 mentions), particularly in relation to national security, disinformation campaigns, and diplomatic sabotage.
- Healthcare, E-commerce, and Retail (2–3 mentions each), noted for their exposure to identity fraud and customer impersonation.

Other sectors mentioned included law enforcement, education, insurance, infrastructure, entertainment, and military, each appearing in multiple responses. Less frequently cited but still relevant were marketing, tech industry, social media, etc. Overall, the responses suggest that deepfake threats are perceived as cross-sectoral, with particular concern for industries handling sensitive data, public communications, and financial transactions.

5.4.8. Advice

Responses (from 49 participants) to the question regarding advice for forensic professionals dealing with deepfake-related cases revealed several recurring themes.

- **Education and training:** Many respondents emphasised the importance of staying informed through ongoing research, reading literature, and keeping up with technological developments.
- **Tool usage:** A significant number advised using detection tools cautiously, verifying file origins, and employing technologies to assess authenticity.
- **Metadata analysis:** Several responses highlighted the value of examining metadata and timestamps to identify inconsistencies and support validation.
- **Critical thinking:** Practitioners were encouraged to question the authenticity of media, rely on common sense, and avoid trusting any single source without verification.
- **Collaboration:** Some respondents stressed the need for sharing findings, collaborating with peers, and educating stakeholders, including clients and legal teams.
- **Uncertainty:** A portion of participants expressed uncertainty or noted they lacked sufficient experience to offer advice.

Consensus from the community is that the forensic processes must adhere to rigorous standards to ensure reliability and admissibility of evidence. However, practitioners currently face a lack of formalised guidance or universally accepted protocols. In the absence of established frameworks, many rely on trial-and-error approaches, which can lead to inconsistencies in methodology and outcomes. This gap underscores the urgent need for collaborative efforts to develop standardised procedures or SOPs (standard operating procedures), particularly as the complexity

and prevalence of deepfakes continue to rise.

5.4.9. Anything else?

The analysis of the final open-ended question, *"Is there anything else you would like to add?"*, revealed several recurring themes, offering deeper insight into professional concerns surrounding deepfakes.

'Lack of tools and standards' emerged as a prominent theme. Many respondents voiced concern over the absence of industry recommended and approved tools. Also, the need for standardised methodologies for detecting and managing deepfakes. This was often linked to a perceived gap in both academic literature and practical guidance, suggesting a need for more structured approaches within the field.

'Concerns about AI reliability' were also frequently mentioned. Participants highlighted the limitations of current AI technologies, particularly the risk of false positives or negatives in forensic contexts. There was a clear call for explainable AI (XAI) that can withstand legal and professional scrutiny, reinforcing the importance of transparency and accountability in automated decision-making.

'Industry vulnerability' was another recurring issue, with finance, banking, and e-commerce identified as sectors most at risk. Respondents viewed deepfakes as an escalating threat to these industries, capable of undermining trust and security in digital transactions and communications. *'Cross-Industry Concern'* was a similar theme, with consensus that deepfakes pose a serious challenge across multiple sectors. Respondents stressed that the issue is not confined to any single domain but rather represents a widespread and evolving risk.

Several responses touched on the *'Emotional and human impact'* of deepfake-related incidents. These included cases involving fraud, indecent media, and reputational damage, with participants reflecting on the psychological toll such events can have on victims and professionals alike. Also highlighting that many cases or incidents could involve deepfake media that could have strong implications before the police and DFUs get involved.

There was also interest in *'Further Research'*, with many respondents expressing appreciation for the survey and a desire to engage in follow-up studies. This indicates a broader appetite for continued exploration and dialogue around the implications of deepfakes. Similarly, the *Need for Training and Continuous Professional Development (CPD)* was noted by a few participants. Keeping up to date with emerging digital threats was seen as essential, underscoring the importance of ongoing education and skill development. Finally, some participants offered *'Verification Advice'*, suggesting practical strategies such as cross-verifying sources and maintaining a healthy scepticism when evaluating digital content.

6. Discussion and Evaluation

This study represents the first comprehensive survey to explore practitioner experiences with deepfake media across diverse sectors, including law enforcement, academia, consultancy, and research. It provides valuable empirical insights into the perceived effectiveness of AI-driven detection tools, while also highlighting practitioner concerns related to legislation, workflow integration, and tool reliability. The findings reveal significant gaps in institutional guidance, training, and preparedness, underscoring the need for stronger collaboration between researchers, practitioners, and policymakers. The resulting dataset (Mac Dermott, 2025b) provides a foundation for further academic analysis and future research.

The evaluation considers each research question in relation to the study's aims and objectives, assessing how effectively they illuminate gaps in forensic practice, technical capability, and institutional readiness.

RQ1: Questions on professional experience and case exposure revealed how deepfakes are influencing forensic workflows. Although only a minority of respondents had encountered deepfake evidence directly, most reported that their organisations lacked formal guidance or legislation on synthetic media. This absence of structured protocols suggests that practitioners are navigating these challenges without adequate institutional support.

RQ2: Demographic and technical questions captured practitioners' familiarity with deepfake technologies, detection techniques, and forensic challenges. While most participants were conceptually aware of deepfakes, detailed technical understanding and confidence in detection methods were limited. This highlights the need for targeted training and clearer operational guidance.

RQ3: Open-ended responses and Likert-scale items highlighted concerns about tool reliability, lack of standardised processes, and insufficient training resources. While some practitioners expressed optimism about AI-driven detection tools, most questioned their accuracy and real-world applicability, pointing to a need for improved validation and transparency.

The overall demographic analysis of survey respondents indicates a highly qualified and professionally diverse group, predominantly composed of experienced individuals working in digital forensics and cybersecurity. The demographic profile reflects a well-informed and experienced practitioner base, providing credibility to the survey findings and ensuring that the insights gathered are grounded in real-world forensic and cybersecurity practice. *'Digital forensic consultant'*, *'Cyber consultant'*, and *'Law enforcement/government agency'* made up 51 % of respondents, with 10 % as *'Other'*. For future surveys, allowing participants to specify their exact role would ensure that categories accurately reflect their professional positions.

The analysis reinforces the view that deepfake and synthetic media represent an emerging threat requiring greater attention, targeted training, and advanced tool development within digital forensic and cybersecurity workflows. Notably, 86 % of respondents reported that their employer either lacked guidance or legislation on deepfakes, or they were unaware of such measures. This absence of formal direction indicates that many professionals are navigating these challenges without structured support, policies, or training. Consequently, there is an urgent need for organisations to implement clear protocols, educational resources, and legal frameworks to enable effective responses to deepfake-related incidents.

Overall, the findings highlight the critical importance of developing robust detection tools, establishing standardised processes, and fostering interdisciplinary collaboration to address the growing threat of deepfakes in professional contexts. While some practitioners expressed optimism about AI-driven detection solutions, the majority questioned their reliability and real-world applicability, underscoring the need for improved accuracy, transparency, and rigorous validation.

Deepfake technologies further challenge traditional forensic methods by introducing highly convincing synthetic content capable of evading standard verification techniques. This creates a pressing need to update the literature to reflect the evolving nature of multimedia manipulation, integrating deepfake-specific methodologies into broader forensic frameworks. Strengthening this connection will not only enhance technical understanding but also support the development of more cohesive tools, training, and policy responses across sectors.

Moreover, the relationship between deepfake analysis and multimedia forensics requires clearer articulation within academic and professional literature. While both fields share a focus on the authentication and integrity of digital media, current literature often treats them as separate domains, resulting in fragmented approaches to detection and

response. Addressing this gap is essential for creating unified strategies that advance forensic practice and policy development.

6.1. Limitations

While the survey aimed to protect participant privacy by avoiding the collection of personally identifiable information, this approach introduced certain analytical constraints. Notably, it limited the ability to assess regional needs and identify patterns or cases specific to geographic areas. Additionally, the level of response varied across questions, with some items receiving more detailed input than others. A few questions were occasionally misunderstood, which may have affected the consistency and clarity of the data collected.

Another limitation is the predominantly UK-based respondent pool, which may introduce jurisdictional bias. Legal frameworks, organisational policies, and investigative practices differ across regions, meaning the findings may not fully reflect global perspectives. Future research should aim to collect a more geographically diverse sample and incorporate regional mapping to link responses to specific jurisdictions. This would provide richer context and enable comparative analysis of legislative and operational approaches to deepfake forensics internationally. Also, despite being circulated through professional networks, the overall uptake of the survey was less extensive than anticipated, suggesting that further engagement strategies may be needed to reach a broader and more representative sample in future studies.

7. Conclusion and recommendations

The findings of this study highlight the growing complexity of media manipulation and the urgent need for enhanced awareness and preparedness among forensic professionals. While the survey provides valuable insights into current practitioner experiences and concerns, it also exposes critical gaps in training and institutional support. To effectively counter the evolving threat of deepfakes and other synthetic media, greater emphasis must be placed on educating police officers, forensic analysts, and investigators about the full spectrum of media manipulation. This includes not only technical detection methods but also best practices for multimedia forensic analysis, ensuring professionals can assess digital evidence with accuracy, confidence, and legal defensibility.

7.1. Recommendations

Enhanced Training for DFUs: DFUs should receive enhanced training on both the creation and detection of deepfakes, including practical exposure to current tools and techniques. This training should also deepen understanding of the various forms that deepfake and fabricated media can take, alongside guidance on the most effective methods for assessing media authenticity and integrity. Enhancing practitioner awareness will enable faster detection and more accurate identification of manipulated content. Incorporating demonstrable use cases across diverse investigative scenarios can further reinforce learning and ensure applicability in real-world contexts.

Development of Forensic Process Models and SOPs: Organisations should prioritise the creation of standardised forensic process models and clear SOPs for handling synthetic media cases. These frameworks will provide structured guidance for practitioners, ensuring consistency, legal defensibility, and adherence to best practices across investigations. SOPs should cover evidence acquisition, validation, reporting, and integration of detection tools within established workflows.

Improving Tool Reliability and Explainability: Existing deepfake detection tools face several limitations, including inconsistent outputs, varying interpretations of results (e.g., AI-generated or not), and reliance on stock data or specific training sets. Explainability is critical in digital forensics to ensure the reliability, trustworthiness, and accountability of AI-based tools. Integrating XAI into forensic workflows can provide clear, interpretable detection decisions, enhancing their practical utility in investigations and strengthening their evidential value in court. Some tools, such as Magnet Verify, exemplify this approach by performing structural analyses of media files (assessing origin and provenance, identifying manipulations), delivering explainable findings that support examiners in presenting robust, defensible conclusions.

Acknowledgements

Thank you to all survey respondents and those who had discussions about the content and themes.

Appendix

Table 2
Deepfakes could be a problem in your job role $n = 35$

Theme	Keywords from responses	Count
Social/political manipulation	misinformation, disinformation, political, social media, manipulate public	7
Media manipulation/fabrication	image, face swap, fake photo, fabricated, generated media, AI-generated, malicious code, metadata	5
Cyber security risks	phishing, spear phishing, vishing, identity fraud, password reset, cybersecurity	5
Authentication risks	authentication, spoofing, access, impersonation	4
Criminal use/threats	revenge pornography, child sexual abuse, blackmail, fraud, money laundering, crime, intimidate	4
Impact on forensic practice	forensics, media provenance, analysis, workflow, backlog, court, investigation	4
Education challenges	student, assessment, academia, education, CPD, fake credentials	4
Legal/judicial concerns	juror, reasonable doubt, court, internal investigation	2
Tool reliability/detection	low quality, high quality, metadata, detection, tool, identify	1

Table 3
Approximately how many cases/incidents have you been involved in that required analysis of deepfake media? $n = 46$

Cases/Incident Amount	Count
0	21
1	1
2	3
3	1
4	1
10	1
Cases/Incident Amount	**Count**
Minimal exposure	4
Moderate exposure	2
High exposure	1
Research context only	1
Increasing exposure	1
Social media observation	1
Not relevant to role	4
Easy detection	1
Obvious to naked eye	1
Detection comments	1

Data availability

Data is available and linked in the article.

References

Breitinger, F., Hilgert, J.-N., Hargreaves, C., Sheppard, J., Overdorf, R., Scanlon, M., 2024. DFRWS EU 10-Year review and future directions in digital forensic research. Forensic Sci. Int.: Digit. Invest. 48.

Garfinkel, S.L., 2010. Digital forensics research: the next 10 years. Digit. Invest. 7 (S1), S64–S73.

Hargreaves, C., Breitinger, F., Dowthwaite, L., Webb, H., Scanlon, M., 2024. DFPulse: the 2024 digital forensic practitioner survey. Forensic Sci. Int.: Digit. Invest. 51. https://doi.org/10.1016/j.fsidi.2024.301844.

Interpol, 2024. Beyond illusions: unmasking the threat of synthetic media for law enforcement. INTERPOL. https://www.interpol.int/content/download/21179/file/BEYOND%20ILLUSIONS_Report_2024.pdf.

Lewis, A., Vu, P., Duch, R.M., Chowdhury, A., 2023. Deepfake detection with and without content warnings. R. Soc. Open Sci. 10 (12), 231214. https://doi.org/10.1098/rsos.231214.

Lyle, J.R., Guttman, B., Butler, J.M., Sauerwein, K., Reed, C., Lloyd, C.E., 2022. Digital Investigation Techniques: A NIST Scientific Foundation Review (NIST Internal Report 8354). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8354.

Mac Dermott, Á., 2025b. Deepfake Forensic Survey Dataset. Liverpool John Moores University. https://doi.org/10.24377/LJMU.d.00000248. Dataset available via JISC. LJMU Ethics Approval Reference: 25/CMP/004.

MacDermott, Á., 2025a. Deepfake forensics: exploring the impact and implications of fabricated media in digital forensic investigations. In: Poster Presented DFRWS EU 2025 Brno, Czech Republic, April https://dfrws.org/wp-content/uploads/2025/04/DFRWS_EU_2025_paperposter_115.pdf.

Qureshi, S.M., Saeed, A., Almotiri, S.H., Ahmad, F., Al Ghamdi, M.A., 2024. Deepfake forensics: a survey of digital forensic methods for multimodal deepfake identification on social media. PeerJ Comput. Sci. 10, e2037.

Sanchez, L., Grajeda, C., Baggili, I., Hall, C., 2019. A practitioner survey exploring the value of forensic tools, AI, filtering, & safer presentation for investigating Child sexual abuse material (CSAM). Digit. Invest. 29, S142–S150. https://doi.org/10.1016/j.diin.2019.04.005.

Silva, S.H., Bethany, M., Votto, A.M., Scarff, I.H., Beebe, N., Najafirad, P., 2022. Deepfake forensics analysis: an explainable hierarchical ensemble of weakly supervised models. Forensic Sci. Int.: Synergy 4, 100217.

U.S. Department of Homeland Security, 2023. Increasing Threats of Deepfake Identities. Washington, D.C.DHS. Availce at: https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.