LIVERPOOL JOHN MOORES UNIVERSITY

DFRWS 2026 EUROPE

Ctrl+Alt+Deceit: Policing the Deepfake Dilemma

A Practitioner Survey on the Impact and Challenges of Synthetic Media Forensics

Dr Áine MacDermott
Senior Lecturer in Cyber Security and Digital Forensics
School of Computer Science and Mathematics

Outline

- Background on the problem
- Deepfake Forensics Survey
- Results, Analysis and Evaluation
- Conclusions and Recommendations
- Q&A

Rise in Deepfakes

- The rapid rise of deepfake technology is reshaping how authenticity and trust are established in digital evidence! The '*deepfake defence'* and questions over media are adding an extra level of scrutiny to file analysis.

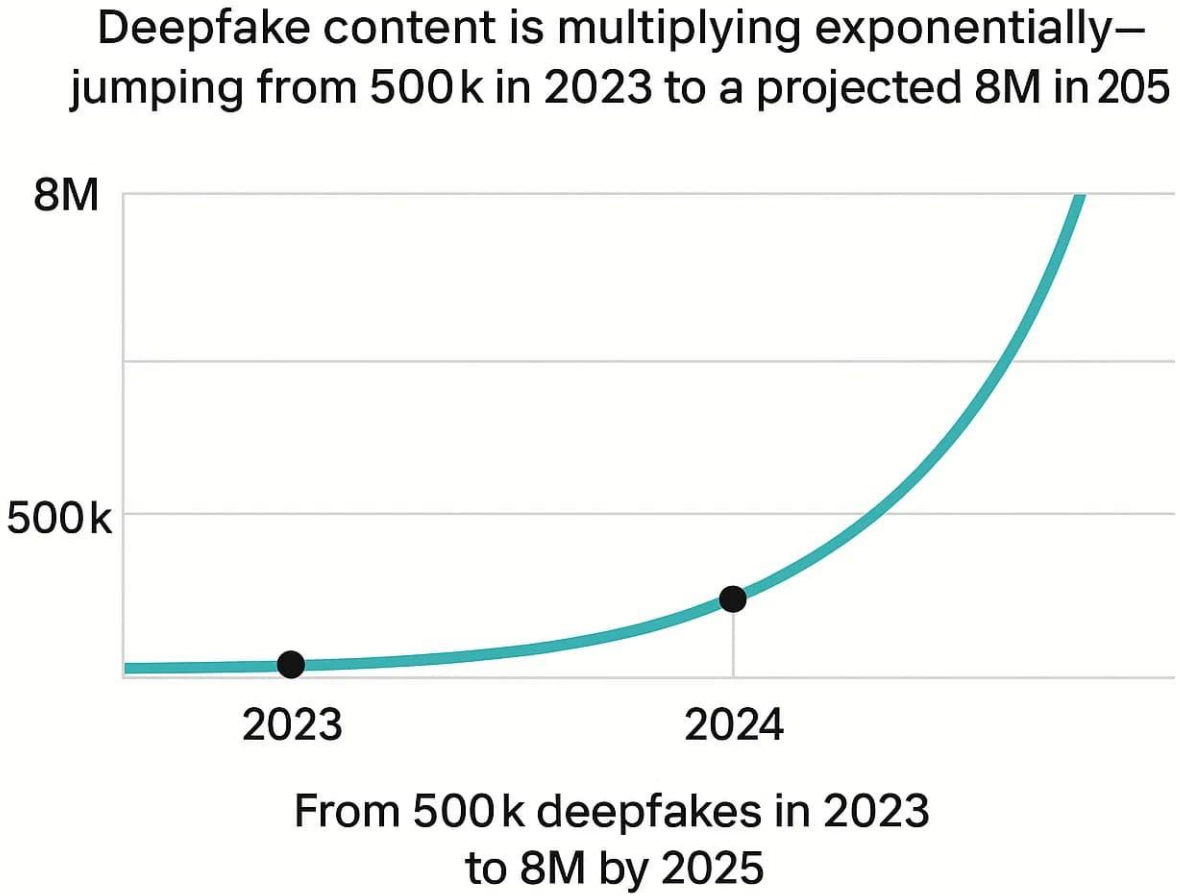
- **Deepfake forensics** refers to the field of study and practice focused on detecting, analysing, and understanding synthetic media (particularly deepfakes) using digital forensic techniques.
  - It combines elements of computer science, digital forensics, machine learning, and multimedia analysis to identify whether audio, video, or images have been artificially generated or manipulated.

Deepfake Frequency

- Deepfake technologies are advancing rapidly, and so are the methods used to evade detection. Forensic techniques must adapt just as quickly, often requiring researchers and practitioners to stay ahead of the curve in what has become a technological arms race.

- The frequency and use-cases of deepfake media in forensic investigations is rising. The time spent analysing a suspect deepfake to confirm the validity of the media in more time consuming than non-deepfake and the availability/accuracy of tools can vary.

Deepfake Frequency



Related Work

- Foundational research (Garfinkel 2010; Lyle et al. 2022; Breitinger et al. 2024) has mapped key digital forensic challenges (including tool validation, reproducibility, and methodological limitations) while highlighting the need for stronger scientific foundations.

- Practitioner-focused studies (Sanchez et al. 2019; Hargreaves et al. 2024) reveal gaps in tool evaluation, training, workflow efficiency, and the uptake of academic research, offering insight into real-world forensic environments and priorities.

- Recent practical guidance from Interpol (2024) and the U.S. Department of Homeland Security (2023) emphasises the growing risks of deepfakes and the need for multi-layered mitigation strategies combining technical solutions, education, and policy.

Practitioner Survey

- 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.

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?

Aims and Objectives

The overarching aim of this study was 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 usable statistics and produce an anonymised dataset, enabling researchers and the academic community to conduct further analysis and advance the field of synthetic media forensics.

Deepfake Forensics Survey

Deepfake Forensics Survey Data

Mac Dermott, Aine (2025) **Deepfake Forensics Survey Data.** [Data Collection]

Copy

How to cite this Dataset

Mac Dermott, Aine (2025) *Deepfake Forensics Survey Data.* [Data Collection]

Abstract

The dataset presented here originates from the Deepfake Forensic Survey conducted between March and October 2025. It includes raw responses, preliminary analysis, and visual representations such as bar charts to illustrate key findings.

Download

Text
Readme_.txt - Full Archive
Available under License Creative Commons Attribution.
Download (3kB)

Archive
Deepfake Forensics Survey Data.zip - Data
Available under License Creative Commons Attribution.
Download (289kB)

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

Available at: https://opendata.ljmu.ac.uk/id/eprint/248/

Demographic overview *n* = 59

Gender	*n*	%
Female	14	24%
Male	40	68%
Prefer not to say	5	8%

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%
CPD	1	2%

Country	*n*	%
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%

Current Role

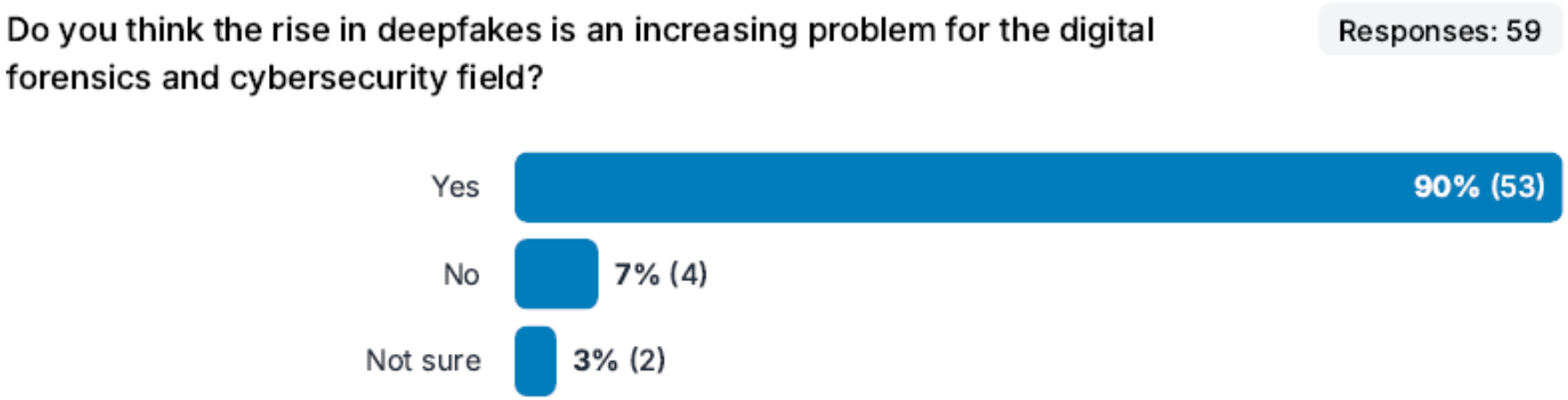
- Participants were asked to specify their current professional roles:
  - Academic/Lecturer (*n=17*, 29%)
  - Law enforcement or government agencies (*n=13*, 22%)
  - Cyber consultants (*n=11*, 19%)
  - Researchers (*n = 6*, 10%)
  - Digital forensic consultants (*n=4*, 7%)
  - Students (*n=2*, 3%)
  - Other (*n=6,* 10%)

A diverse range of roles within the digital forensics and cybersecurity landscape ☺

Insights

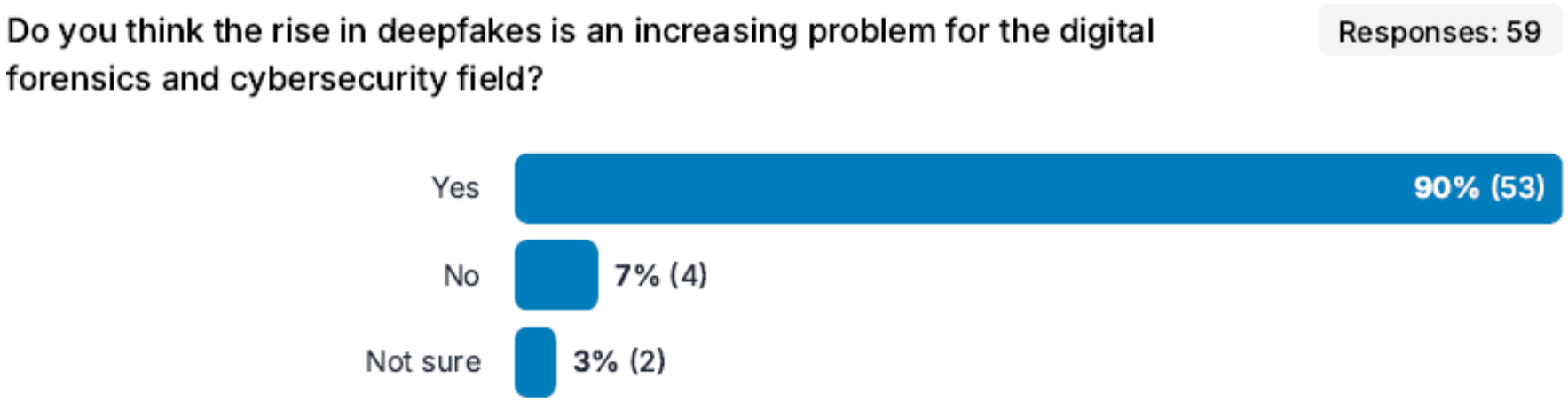
- Exploring the impact and implications of deepfakes/fabricated media in digital forensic investigations and the cyber domain.

- 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 voted Yes:



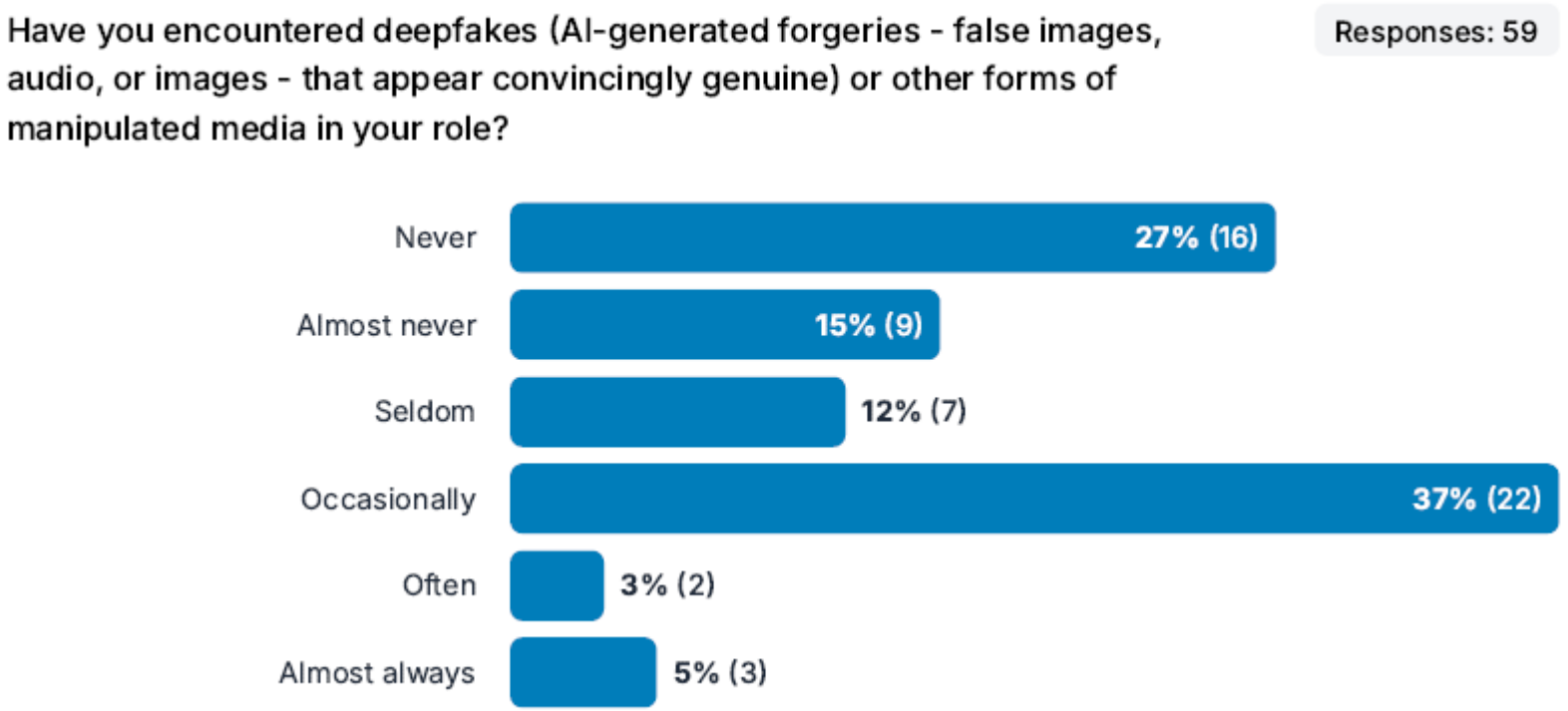
Insights: Deepfake Problem?

- 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 voted Yes:



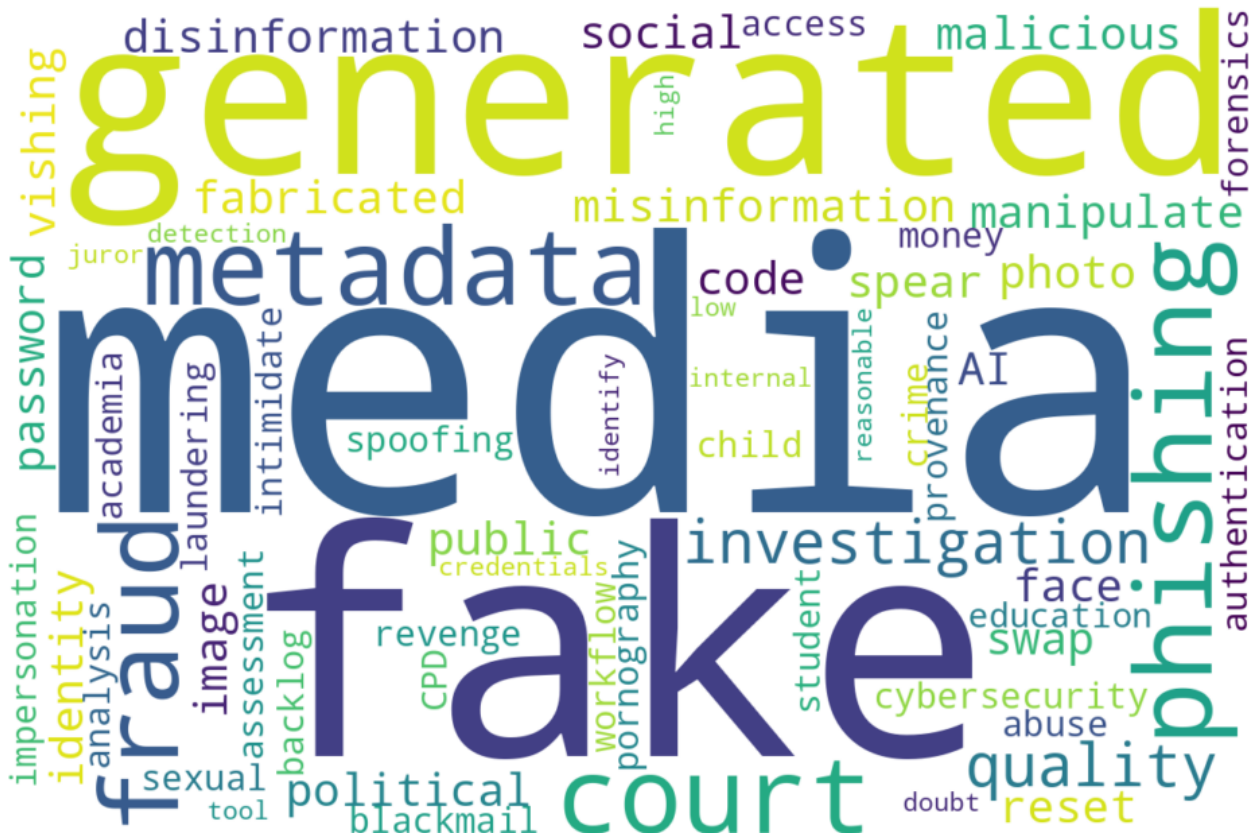
Deepfake Encounters

- 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:



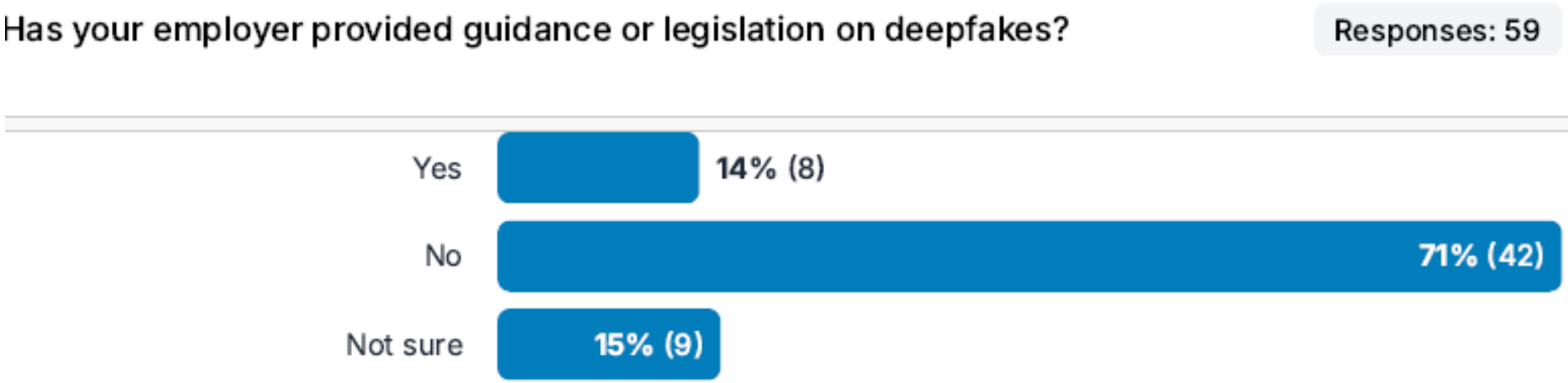
Deepfake Encounters

- If yes, please give an example of how deepfakes could be a problem in your job role *(n = 35):*



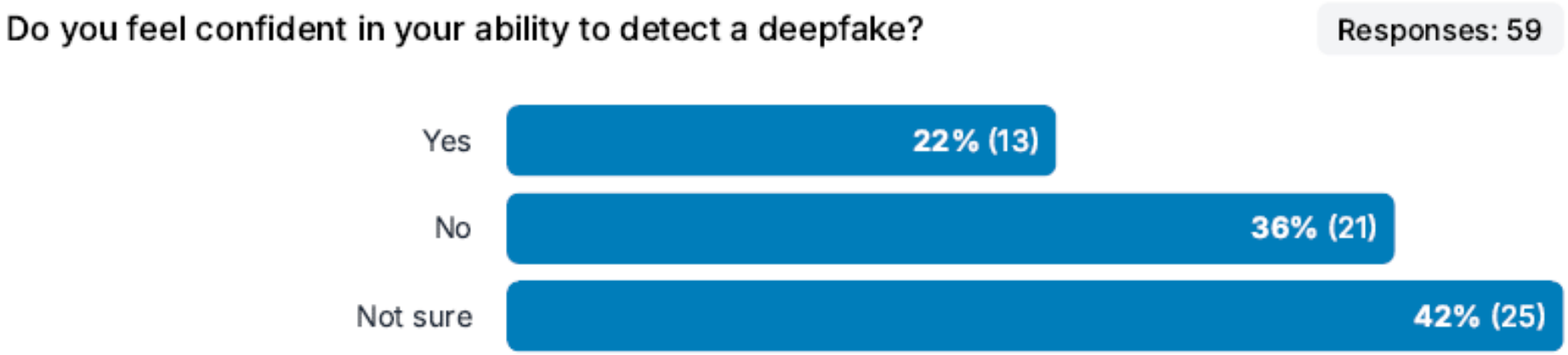
Guidance or legislation

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



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.



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.

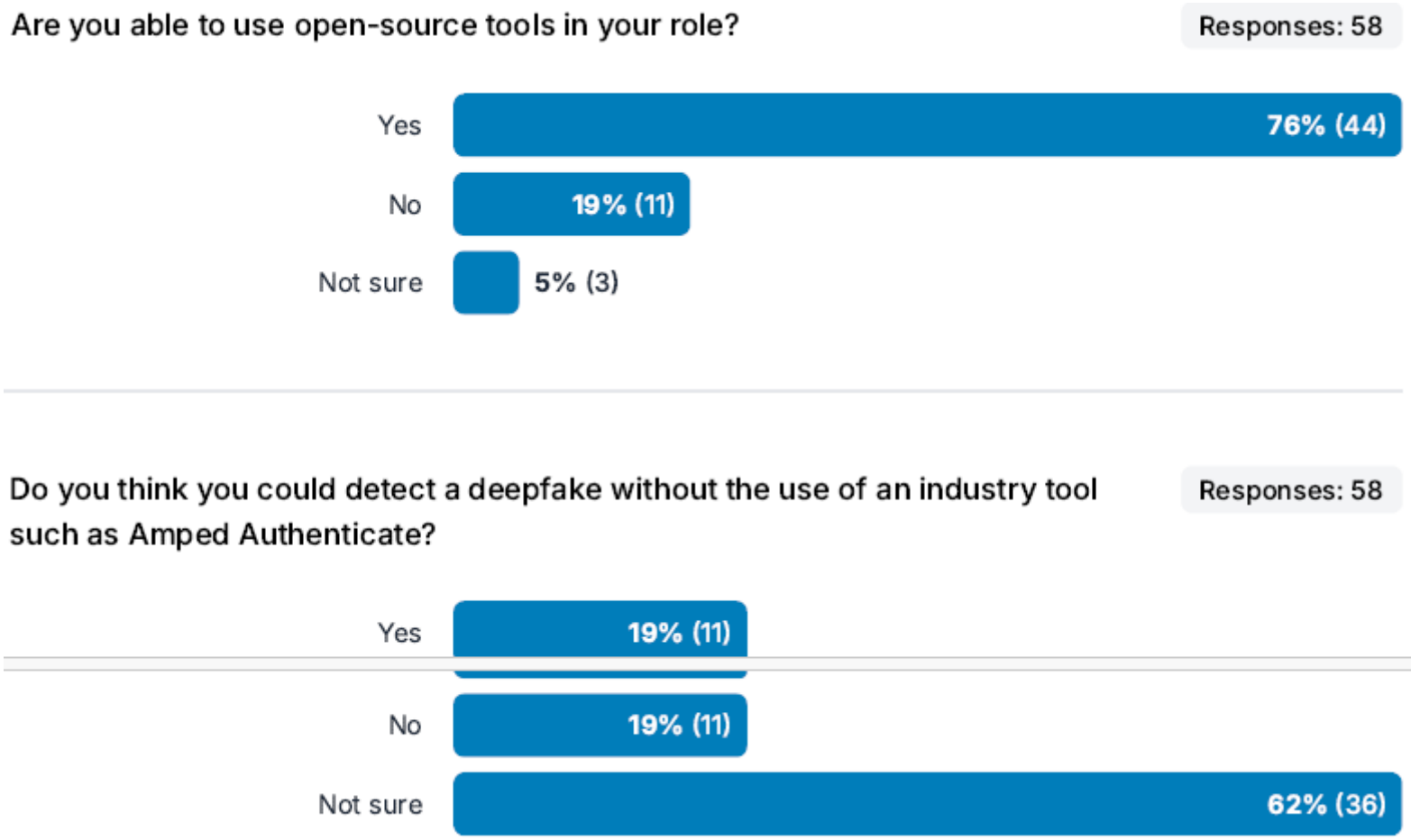
Cases/ Incidents	Count
0	21
1	1
2	3
3	1
4	1
10	1

Cases/ Incidents	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

Effectiveness of tools (*n = 57)*

- **Not Effective**: 14 respondents expressed skepticism about 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.
- **Mixed/Variable**: 6 responses highlighted that effectiveness depends on the tool, context, or case, reflecting inconsistency across available solutions.

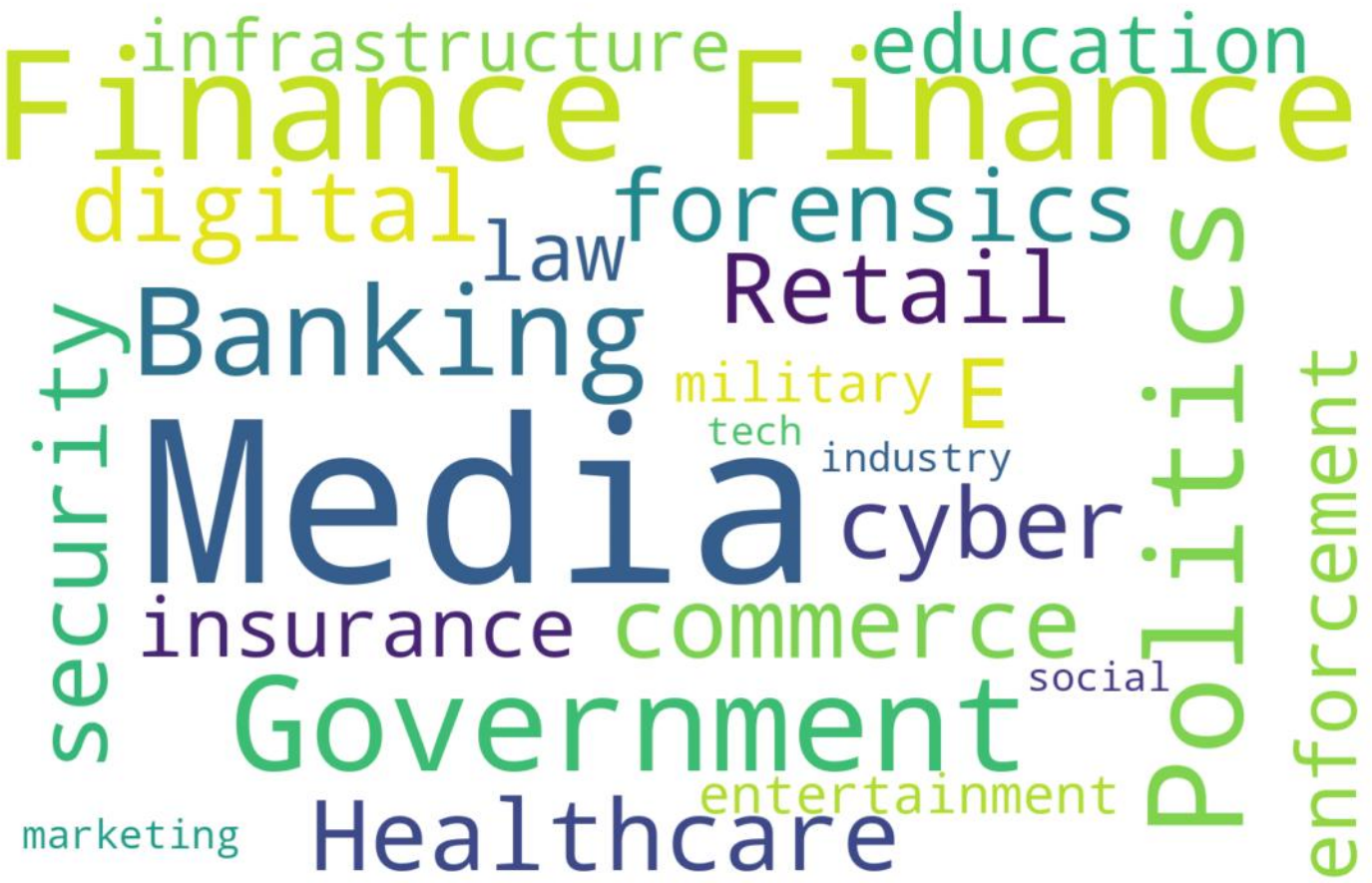
Effectiveness of tools



LIVERPOOL JOHN MOORES UNIVERSITY

Vulnerable Sectors (*n=51)*

DFRWS 2026EUROPE



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 ad hoc/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.

Anything else?

- 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.
  - Concerns about AI reliability and 'industry' tools
  - Perceived gap in both academic literature and practical guidance, suggesting a need for more structured approaches within the field.
  - Industry vulnerability/Industry concern/Further research
  - 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.

Evaluation

- **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.

Evaluation

- **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 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.

- For future surveys, allowing participants to specify their exact role would ensure that categories accurately reflect their professional positions.

Evaluation

- 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.

Deepfake Definitions

- 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.
- The relationship between deepfake analysis and multimedia forensics requires clearer articulation within academic and professional literature.

Limitations

- While the survey aimed to protect participant privacy by avoiding the collection of personally identifiable information, this approach introduced analytical constraints. Notably, it limited the ability to assess regional needs and identify patterns or cases specific to geographic areas.

- The level of response varied across questions, with some items receiving more detailed input than others. A few questions were occasionally misunderstood, which affected consistency and clarity of some data collected.

- 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).

Conclusions

- 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.

Recommendations

- **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.

- **Enhanced training for DFUs** on both the creation and detection of deepfakes, including practical exposure to current tools and techniques.

- **Development of forensic process models and SOPs** for handling synthetic media cases. SOPs should cover evidence acquisition, validation, reporting, and integration of detection tools within established workflows.

Recommendations

- **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.

Thank you for listening ☺

Any questions?

a.m.macdermott@ljmu.ac.uk

Forthcoming book: Áine MacDermott (2026). The Deepfake Dilemma: Technology, Truth, and Forensic Integrity, Taylor & Francis Ltd, CRC Press.