OPEN ACCESS
OPUS AUGSBURG

Universität Augsburg
Universitätsbibliothek

# DFPulse: the 2024 digital forensic practitioner survey

**Christopher Hargreaves, Frank Breitinger, Liz Dowthwaite, Helena Webb, Mark Scanlon**

**Angaben zur Veröffentlichung / Publication details:**

Hargreaves, Christopher, Frank Breitinger, Liz Dowthwaite, Helena Webb, and Mark Scanlon. 2024. "DFPulse: the 2024 digital forensic practitioner survey." Forensic Science International: Digital Investigation 51: 301844. https://doi.org/10.1016/j.fsidi.2024.301844.

**Nutzungsbedingungen / Terms of use:** **CC BY 4.0**

Dieses Dokument wird unter folgenden Bedingungen zur Verfügung gestellt: / This document is made available under these conditions:
**CC-BY 4.0: Creative Commons: Namensnennung**
Weitere Informationen finden Sie unter: / For more information see:
https://creativecommons.org/licenses/by/4.0/deed.de

Forensic Science International: Digital Investigation 51 (2024) 301844

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

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

# DFPulse: The 2024 digital forensic practitioner survey

Christopher Hargreaves [a,*], Frank Breitinger [b,*], Liz Dowthwaite [c,*], Helena Webb [c,*], Mark Scanlon [d,*]

[a] Department of Computer Science, University of Oxford, United Kingdom
[b] School of Criminal Justice, University of Lausanne, Switzerland
[c] School of Computer Science, University of Nottingham, United Kingdom
[d] Forensics and Security Research Group, School of Computer Science, University College Dublin, Ireland

ARTICLE INFO

*Keywords:*
Digital forensics
Practitioner survey
Challenges
Future directions
Artificial intelligence

ABSTRACT

This paper reports on the largest survey of digital forensic practitioners to date (DFPulse) conducted from March to May 2024 resulting in 122 responses. The survey collected information about practitioners' operating environments, the technologies they encounter, investigative techniques they use, the challenges they face, the degree to which academic research is accessed and useful to the practitioner community, and their suggested future research directions. The paper includes quantitative and qualitative results from the survey and a discussion of the implications for academia, the improvements that can be made, and future research directions.

## 1. Introduction

In 2007, Sremack wrote that, in most fields, researchers address issues that practitioners encounter, while practitioners depend on researchers for solutions. If practitioners do not utilise the work of researchers, the researchers' contributions become less relevant. Therefore, researchers must understand the needs and objectives of practitioners to ensure that they are tackling the right problems. This is especially important in digital forensics, where there can be a significant disparity between the needs of practitioners and the goals of researchers. A decade later, Baechler (2017) added that, specifically with respect to policing, the academic and law enforcement (LE) communities are often seen as distinct and disconnected, each with its own goals, values, methods, and procedures. However, it is suggested that better mutual understanding and collaboration between these two spheres are essential to enhance education, professional practice, and research in their respective fields.

This paper reports on a survey conducted targeting digital forensic practitioners to provide data to understand their operating environment, the technologies they encounter and the challenges they face, and also to investigate the extent to which practitioners are engaged in academic research outputs and venues. The purpose of this survey is to better understand the needs of practitioners and to explore the interaction between digital forensic practitioners and researchers, and to identify ways to improve both the relevance of academic work to practitioners and the flow of information between the digital forensic researcher and practitioner communities.

This paper makes the following contributions:

- The design and execution of the most comprehensive survey of digital forensic practitioners to date, with 122 worldwide respondents.
- The responses are analysed across different demographics, providing insight into practitioners' workplace environments, case loads, technologies used and encountered, challenges faced, and future research suggestions.
- Reflections on results, discussion, and practical suggestions for improvements to digital forensic research directions, academic collaboration, and practitioners' engagement with academic output. This includes insights on how a future survey could be further refined.
- A dataset containing the responses to the survey, allowing researchers and the academic community to further analyse and inform their future research directions (https://doi.org/10.5281/zenodo.13612567).

The remainder of the paper is structured as follows: related work is described in Section 2, followed by the design methodology for this sur-

* Corresponding authors.
*E-mail addresses:* christopher.hargreaves@cs.ox.ac.uk (C. Hargreaves), frank.breitinger@unil.ch (F. Breitinger), Liz.Dowthwaite@nottingham.ac.uk (L. Dowthwaite), Helena.Webb@nottingham.ac.uk (H. Webb), mark.scanlon@ucd.ie (M. Scanlon).
*URL:* https://fbreitinger.de (F. Breitinger).

https://doi.org/10.1016/j.fsidi.2024.301844
Received 2 September 2024; Received in revised form 6 November 2024; Accepted 23 November 2024
Available online 29 November 2024
2666-2817/© 2024 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

vey in Section 3. Sections 4 to 7 describe the results, with a discussion of key findings in Section 8. Section 9 describes limitations and potential further work, and Section 10 provides conclusions, including some actionable points to improve collaboration between academia and the practitioner community.

## 2. Previous work

Attempts to improve the digital forensics research programme have been ongoing since the early years of digital forensics. Palmer et al. (2001) produced a report that was the collective output of the first Digital Forensics Research Workshop (DFRWS) in 2001, with 50 university researchers, computer forensic examiners, and analysts in attendance. This collaborative document between academia and practitioners provided the result of a discussion of several topics, including a framework for digital forensic science.

Over the years, others have considered the state of digital forensic research, analysed trends, and predicted future directions. Garfinkel (2010) provided a history of digital forensics and commented on the research challenges at that time, with reflections discussed in Garfinkel (2022). More recently, Breitinger et al. (2024) provided a review of the 135 peer-reviewed articles from the first 10 years of the DFRWS EU research conference and extrapolated trends and suggested future directions.

These more recent publications differ from the earlier work in Palmer et al. (2001), in that they do not have the same involvement of the practitioner community – who are ultimately the ones conducting digital forensic investigations and face practical challenges.

There have been previous surveys of the practitioner communities. Airlie et al. (2021) surveyed 544 forensic scientists worldwide, but the survey's focus does not include digital forensics specifically - this is combined in the category of "other" in the survey alongside several other traditional forensic disciplines.

Some other surveys have focused on digital forensics or related communities. Al Fahdi et al. (2013) surveyed 23 practitioners covering demographics, current capabilities, future challenges, and legislative concerns. The findings included that the limitations of the identified tools were in handling the volume of data and the time taken. They also noted that more than double the proportion of researchers (63%) felt that automation of forensic analysis was a limitation compared to practitioners (30%). This suggests the potential for differences in options between researchers and practitioners. It also discussed potential future challenges (from anti-forensics through to visualisation), with anti-forensics, cloud computing, and encryption ranking the highest.

Gurule (2016) investigated whether having a specialised cybercrime unit increase efficiency and effectiveness in law enforcement agencies (LEAs) and undertook phone interviews and an online survey. Survey data was obtained for 16 units (both specialist and non-specialist) throughout the US, including: number of cases, phones, disks and other media examined, and the time spent on each case type. This also collected other investigative statistics, such as the number of leads reported to the National Center for Missing and Exploited Children (NCMEC) or to Internet Crimes Complaints Center (IC3). Other high-level information was also obtained, such as year established, certifications, tools used, number of personnel, including a breakdown of LE vs. civilian personnel.

Luciano et al. (2018) conducted a workshop to discuss with 24 digital forensics experts (16 from academia), and analysed the resulting qualitative and quantitative data from participants to identify issues, future directions, necessary improvements, anticipated challenges, and key research opportunities in the next five years.

Other studies have also focused on specific research areas, e.g. skills of incident response practitioners and a skills map of gaps in education (33 responses) (Hranickỳ et al., 2021), and the psychological well-being and coping mechanisms of those investigating child abuse cases (129 responses) (Seigfried-Spellar, 2018). The latter found that 20% of the respondents knew someone who has sought counselling or treatment as a result of working on child abuse cases. This topic was also covered in Sanchez et al. (2019) (106 responses) including tools used to assist in the process.

Larsen et al. (2023) investigated the study, and subsequent use, of Open Source Intelligence (OSINT) techniques during their training at the Norwegian Police University College (NPUC) (521 responses), and Vasilaras et al. (2024) conducted a 13-question survey on the use of AI in mobile phone investigations (37 respondents) with questions regarding their accuracy and usefulness, followed by a separate case study computing evaluation metrics for several tools.

Some reports come directly from practitioners, e.g. the Department of Justice (DOJ) Regional Computer Forensic Laboratory (RCFL) annual reports from 2003 to 2023 (RCFL, 2024) include reports from 17 laboratories providing coverage to 23 US states. For example, in 2023, the report included statistics on the number of on-site searches conducted (682), court testimonies (108), and service requests received. It also provides the top five crimes for each region and short case studies of specific investigations. The reports also provide goals for the next financial year and report on the progress towards goals in the current one.

In the UK, the Digital Forensic Science Strategy (Forensic Capability Network UK, 2020) provides a discussion of many of the challenges faced, including three core challenges (volume, complexity, and legitimacy), and seven issues (lack of support services, fragile commercial marketplace, limited strategic engagement with partners (academia and industry) to work on long-term solutions, recruitment and retention, lack of awareness of digital forensic science within police, embedding quality, and handling legacy data).

In summary, while academic efforts have been made to define research challenges, they are often based on existing academic work and lack practitioner input. There have been several surveys conducted, but all have either not been focused on digital forensics, or have had limited scope, or have had limited responses. There are some publications direct from policing, but they do not provide sufficient technical operational details that would be useful in prioritising specific research, nor do they focus on the relationship between academia and practitioners. This survey aims to fill the gaps left by the existing work.

## 3. Methodology

### 3.1. Survey design

This survey consists of three sections and was completed by respondents using a multi-page Google Form (a copy of which is available at the dataset link). The first part of the survey focused on demographics, which consisted of 19 questions. In addition to typical demographic questions such as gender, education, and role, this section also included questions about the expertise of participants, individual workload, laboratory workload, time allocated for training and research, and the use of open source tools.

The second part of the survey focused on the current work of the respondents and the challenges they face. This section consisted of 19 questions, some of which were optional, inviting additional input to closed-ended questions to ensure comprehensive coverage of potential responses. For example, one multiple choice question asked "Which file systems do you encounter?", followed by a prompt for any additional file systems encountered that were not listed.

The third part of the survey focused on how academic research could be better communicated to practitioners. Its completion was optional, and participants could end the survey after the second part if they wished. Participants who continued received an additional 11 questions that, like before, were mandatory. In total, 96 participants completed this third part.

Ethical approval was granted by the Human Research Ethics Committee in University College Dublin (UCD) with approval number LS-LR-24-110-Scanlon, with the other non-UCD authors also gaining approval

to conduct the study. The final survey included a preamble providing details as to who is conducting the survey, why, how the data will be used, privacy protection measures, data sharing, etc. Participants were asked to explicitly consent to participate in the study and continue the survey.

### 3.2. Promotion and recruitment

The advertisement for survey recruitment was posted online on LinkedIn, X (formerly Twitter), the Digital Forensic Science (DFSci) mailing list, the High Technology Crime Investigation Association (HTCIA) mailing list, the Digital Forensics Discord server and was highlighted on the Digital Forensics Now podcast. It was also promoted as a lightning talk and by distributing flyers at the Digital Forensics Research Conference Europe 2024 (DFRWS EU). In addition, a snowball sampling methodology was used in which recipients were encouraged to share the survey link with colleagues. The survey link was shortened using `bit.ly` (with corresponding QR code) allowing interactions to be monitored. In total, 721 visits were registered during the survey response window (13th March to 20th May 2024) and 122 completed it.

### 3.3. Data cleanup

The results required a small amount of data cleanup. This was achieved by reviewing the responses to ensure that they were consistent with the questions. In cases where obvious mistakes were identified, they were corrected manually, e.g. two participants mistakenly answered the question "How many years ago did you gain this qualification? (please enter a whole number)" with the year they received the degree (i.e., 1994, 2024) instead of the number of years (i.e., 20, 0).

### 3.4. Data analysis

#### 3.4.1. Quantitative analysis

The data was exported from the survey software as a `.csv` file and imported into SPSS 27 for analysis. For all questions, descriptive statistics were extracted, predominantly frequencies for closed-ended questions. The majority of the questions were then converted to numerical (ordinal) scales for further examination. Many questions asked "how often..." where answer possibilities were as follows:

- *almost always (80-100%)*,
- *often (60-80%)*,
- *occasionally (40-60%)*,
- *seldom (20-40%)*,
- *almost never (1-20%)*, and
- *never (0%)*.

For analysis, these responses were numerically assigned between 0 (*never* 0%) and 5 (*almost always* (80-100%)). Several other questions included scales as follows:

- from *0 (no experience)* to *5 (I am an expert)*
- from *0 (not impactful)* to *4 (very impactful)*
- from *1 (very unlikely)* to *5 (very likely)*

For numerical variables, the mean, standard deviation, median, interquartile range (IQR), mode, percentiles (1, 25, 50, 75, 100), skew, and kurtosis were calculated. Most variables showed significant skew and/or kurtosis, indicating that the responses are not normally distributed, so it is more appropriate to use the median in reporting. IQR and percentiles are useful for understanding the spread of responses, with IQR indicating the range within which 50% of responses fall (25-75%). Note that all values are rounded to one decimal place, which may result in some answers or table columns, presented below, not summing to exactly 100%. In some cases, free-text responses were only slightly re-worded versions of the options provided, and these were added to the grouped totals. Three outliers were removed from the training and research responses as they were extremely high and inconsistent with other responses from the same participants. Furthermore, a chi-square test was carried out to examine the difference in opinion on open source software between academic respondents and other respondents, and the difference in case backlogs between law enforcement and other respondents, with a threshold of $p < 0.05$ indicating statistical significance.

#### 3.4.2. Qualitative analysis

For several questions, free text responses were possible. These responses were extracted and analysed using a thematic analysis approach in which responses were grouped according to recurring patterns within them. The themes derived are largely descriptive and seek to highlight the major commonalities and trends within the data without seeking to make claims of exact statistical representativeness.

### 3.5. Presentation of results

The results are reported in the upcoming sections and are grouped by theme, rather than necessarily by question or survey section. Specifically, Sections 4 and 5 map to the questions asked in survey part one, Section 6 maps to the second part of the survey, and Section 7 maps the third part. Some questions are aggregated to improve the readability of this paper.

The results make heavy use of tables and figures, mainly in the form of stacked 100% charts, which best represent the different responses provided by the participants. The sections also provide some discussion and interpretation of the results, with more general conclusions, directions, and recommendations provided in Section 8.

## 4. Results: demographics

The survey included typical demographic questions such as gender, country, education, and time in role. It also included questions about participants' role(s), expertise, and education. The overall profile of the participants is summarised in Table 1, with details discussed in the upcoming subsections.

### 4.1. Gender and country

The majority of participants were male (80.3%), with 17.2% female and 2.5% declining to answer. There were no responses received for the non-binary and other gender options.

The majority of the responses came from the United States (n = 43, 35.2%), followed by the United Kingdom (n = 21, 17.2%) with 23 other countries represented, ranging from 1-8 respondents (0.8%-6.6%). In later discussions, where regional differences are examined, countries are grouped by: US, UK, Europe (n = 23, 28.6%), and Rest of World (n = 16, 13%) to provide reasonable participant sizes per group.

### 4.2. Employment sector

Participants were asked about the roles they have, which included *any* role they occupy, but specifically indicating their primary role. The majority (61.5%) of respondents' primary role was law enforcement/government agency (n = 75), with 18.0% (n = 15) being industry (including CERT/incident response), 10.7% (n = 13) academics, 12.3% (n = 15) independent consultants. An 'other' option was provided that included responses such as private sector, in-house analysts, retired law enforcement, non-profit public workers, and forensic software developer. The participants with the primary role of academic were checked and in later questions they mostly reported conducting between 2 and 150 cases per year, with only one respondent reporting that they worked on 0 cases per year, but did respond as occasionally performing various aspects of the digital investigation process (discussed in Section 4.3).

**Table 1**
Demographics overview, $n = 122$.

| Gender | n | % |
|---|---|---|
| Male | 98 | 80.3 |
| Female | 21 | 17.2 |
| I prefer not to answer | 3 | 2.5 |
| **Country of primary role** | | |
| United States | 43 | 35.2 |
| United Kingdom | 21 | 17.2 |
| Netherlands | 8 | 6.6 |
| International/Cross-border | 7 | 5.7 |
| Canada | 5 | 4.1 |
| France | 5 | 4.1 |
| Germany | 5 | 4.1 |
| Ireland | 5 | 4.1 |
| Indonesia | 3 | 2.5 |
| Switzerland | 3 | 2.5 |
| Italy | 2 | 1.6 |
| South Africa | 2 | 1.6 |
| Other | 13 | 10.7 |
| **Any roles held** | | |
| Law enforcement/Government Agency | 83 | 68.0 |
| Academic | 30 | 24.6 |
| Independent Consultant | 27 | 22.1 |
| Industry CERT/Incident Response | 15 | 12.3 |
| Industry | 15 | 12.3 |
| Student | 9 | 7.4 |
| Others | 5 | 4.1 |
| **Primary role** | | |
| Law enforcement/Government Agency | 75 | 61.5 |
| Independent Consultant | 15 | 12.3 |
| Academic | 13 | 10.7 |
| Industry | 8 | 6.6 |
| Industry CERT/Incident Response | 7 | 5.7 |
| Other | 4 | 3.3 |
| **Highest Education** | | |
| MSc or equivalent | 57 | 46.7 |
| BSc or equivalent | 25 | 20.5 |
| College or equivalent | 18 | 14.8 |
| PhD | 8 | 6.6 |
| High School | 8 | 6.6 |
| Continuous Professional Development | 4 | 3.3 |
| Prefer not to say | 2 | 1.6 |

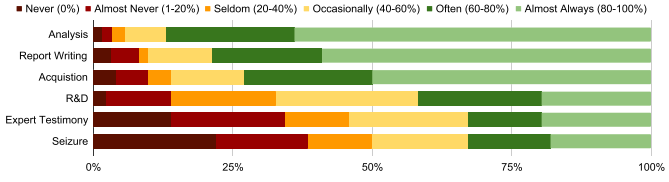


**Fig. 1.** How often participants perform the various stages of a digital investigation. (For interpretation of the colours in the figure(s), the reader is referred to the web version of this article.)

Consequently, these responses were included in the subsequent data analysis.

### 4.3. Digital investigation activities and expertise

Participants were asked how often they performed specific stages of digital investigations, how many cases per year they worked on, along with a self-reporting of their experience in different areas, e.g. mobile forensics, data acquisition, etc. The results are summarised in Fig. 1.

The most frequent aspects of digital investigations that were performed by the participants were: analysis (median = 5.0, IQR = 1.0), report writing (median = 5.0, IQR = 1.0), and acquisition (median = 4.5, IQR = 2.0), with 63.9% (n = 78), 59.0% (n = 72), and 50.0% (n = 61) of participants selecting *almost always* respectively. It is worth noting that only 5.7% (n = 7) responded that they performed the analysis either *never*, *almost never*, or *seldom*, closely mirroring the distribution for responses for report writing.

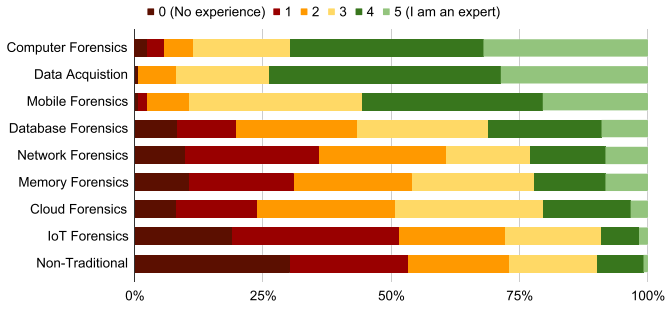


**Fig. 2.** Self-reporting on the level of expertise in areas of digital forensics (sorted in descending order by the proportion that reported *expert*).

There was an interesting discrepancy between those undertaking report writing and giving expert testimony, with 59.0% (n = 72) responding *almost always* to whether they carry out report writing, but only 19.7% (n = 24) reporting the same for giving expert testimony. In terms of how much the respondents were engaged in R&D, the results were much more spread, with *occasionally* being the most frequent answer (25.4%, n = 31, median = 3.0, IQR = 2.0) with similar numbers reporting *seldom* (n = 23, 18.9%), *often* (n = 27, 22.1%), and *almost always* (n = 24, 19.7%).

The responses for undertaking the seizure of devices were also spread, with 22.1% (n = 27) reporting *never* and 18.0% (n = 22) reporting *almost always*. Given that for data to be acquired and analysed, it must be seized in the first place, this may suggest that device seizure or crime scene investigation is a specialist role within digital forensics and that the survey may have failed to reach people in those roles.

In terms of the experience of the participants in digital forensic subdisciplines, e.g. mobile forensics, data acquisition, etc., they were asked "With 0 meaning 'no experience' and 5 meaning 'I am an expert', to what extent would you describe yourself as an expert in the following areas" and the results are depicted in Fig. 2. The results show much higher levels of self-reported expertise in data acquisition (median = 4.0, IQR = 2.0), computer forensics (median = 4.0, IQR = 2.0), and mobile forensics (median = 4.0, IQR = 1.0). Approximately three times the number of participants reported *expert* level abilities in computer forensics (n = 35, 28.7%) compared with database forensics (n = 11, 9.0%), network forensics and memory forensics (both n = 10, 8.2%), and ten times more than cloud forensics (n = 4, 3.3%), IoT forensics (n = 2, 1.6%) and non-traditional devices such as drones, vehicles, etc. (n = 1, 0.8%).

In terms of the caseload of individuals (caseload of the workplace is discussed later), the responses ranged from 0 to 1500 cases per year, with a median of 30.0 (IQR = 54.3); quartiles show that 50.0% of responses fall between 12.0 and 66.3 cases per year. This indicates that while some individuals handle a large number of cases, the typical workload is considerably lower, reflecting variability in individual caseloads and perhaps differences in their investigative work. Note that the survey did not ask about the nature of their participation in those cases, limiting further understanding of the ranges at this time.

### 4.4. Time in role

The survey asked several questions related to the experience of the investigator over time. Participants reported spending between 1 and 40 years in their role (median = 5.0 years, IQR = 7.0), and the same for working in digital forensics (median = 9.0, IQR = 10.0). Quartiles indicate that 50% of the respondents have been in their roles between 2.0 and 9.0 years, and in the field between 5.0 and 15.0 years.

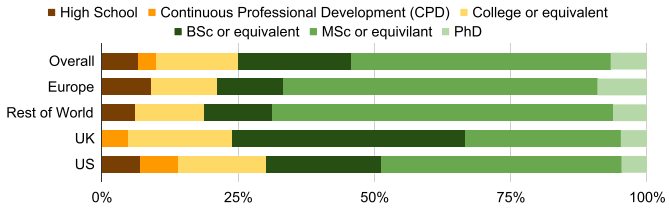


**Fig. 3.** Highest level of qualification by region.

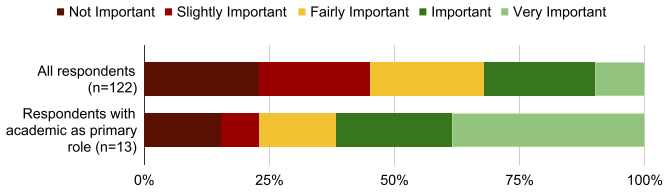


**Fig. 4.** Responses regarding the importance of tools being open source.

### 4.5. Education

The participants were also asked to report their highest level of qualification, and the results are summarised in Fig. 3. Two respondents were excluded because they responded with *prefer not to say*, giving n = 120. The results show that the majority (n = 57, 46.7%) had an MSc or equivalent, 20.5% (n = 25) had a BSc or equivalent, and 6.6% (n = 8) had a PhD, totalling 73.8% (n = 90) with some university level education.

This can also be considered geographically and using the geographic groupings discussed earlier to ensure appropriate size groups, Fig. 3 also shows the breakdown by region. *Rest of World* (81.3%) had the highest level of university education, with the US being the lowest (69.8%). There is also an outlier in the UK, which had similar levels of university education, but with significantly fewer people reporting MSc level qualifications, but much higher BSc level.

It is important to note that given that several of the authors of the survey who were also responsible for disseminating the survey teach or taught Masters level digital forensic courses, there is the potential for bias in these results.

When asked how long ago they received their qualification, the range of responses was between 0 years and 38 years (median = 8.5, IQR = 13) with 50.0% of responses between 4 and 17 years.

## 5. Results: workplace environment

Also included within the demographics section of the survey were questions about the operating conditions in which the participants worked, including lab size and lab workload, use of open source tools, time allocated for training, and for research.

### 5.1. Lab size and caseload

To understand the size of the labs, the participants were asked how many people perform investigations in their lab. The responses varied widely, ranging from 0 to 60 investigators, with a median of 5 and an IQR of 11, between 2 and 13. Thus, while some labs are quite large, the majority of respondents had relatively small investigative teams.

Regarding the number of cases handled by labs, the responses ranged from 0 to 4,000 cases per year, with a median of 135 and an IQR of 360, between 40 and 400 cases. This wide range suggests that while a few labs handle a very high volume of cases, most labs work on a significantly smaller number, resulting in a skewed average.

### 5.2. Time available for training

After removing a single outlier, on average, participants reported receiving a median of 10 days of training annually (IQR = 15); five individuals stated that they receive between 50 and 100 days of training each year. Notably, 20.5% of participants indicated the median score (10 days) much more than any other duration.

### 5.3. Time available for research

Two questions addressed the time spent on research. First, participants were asked how much time they spent researching per case. Many responded with 1 hour (n = 19, 15.6%), 2 hours (n = 19, 15.6%), or 5 hours (n = 17, 13.9%). On average, participants spend a median of 5 hours on research per case, with 50.0% between 2 and 10 hours but a maximum of 150 hours. This suggests that while some cases require extensive research, most require significantly less time. The survey also asked about the annual time allocated for research not related to specific cases. After removing two outliers, the results show an average of 91.3 hours per year, with a median of 33.5 hours. This median value, which approximates to just under a week depending on the country, highlights a substantial variation in research time among participants, likely influenced by differences in job roles and organisational support for research activities.

**Table 2**
Indicates the proportion of tools used by participants that are open source.

| Response | n | % |
|---|---|---|
| 0% | 6 | 4.9 |
| 20% | 70 | 57.4 |
| 40% | 22 | 18.0 |
| 60% | 13 | 10.7 |
| 80% | 7 | 5.7 |
| 100% | 4 | 3.3 |

### 5.4. Open source tooling

The survey also asked about the usage of open source tools: “Approximately what proportion of tools that you use for digital forensics are open source?” and “How important is it for the tools you use to be open source?”. The results are shown in Table 2 and Fig. 4.

The number of responses that indicated that open source tools were never used was 4.9% (n = 6), indicating that open source tools are used by a significant portion of the practitioner community, but usually as a small proportion of their tooling. By far, the most common proportion of open source tools in use in labs was 20.0%, reported by 70 participants.

In terms of the importance of open source tools, the responses were mostly evenly distributed across categories: 31.9% (n = 39) indicated that tools being open source was *important* or *very important* (with 9.8% (n = 12) indicating *very important*); 23.0% (n = 28) indicated that it was not important, and an additional 22.1% (n = 27) indicated that it was *slightly important*. This indicates a varied perception of the importance of open source tools among participants.

Interestingly, 13 respondents reported that academia was their primary role. Although the survey was not designed to analyse this specifically, it shows some different response patterns when considered in isolation: significantly more academic respondents considered it very important that the tools were open source (38.5%, n = 5) than everyone else (6.4% n = 7), as shown by a chi-squared analysis, ($X^2(1, 122) = 13.4, p < 0.05$)). The small numbers here make it hard to make conclusive findings, but this potential difference of opinion warrants further investigation in future.

The survey also asked “Which, if any, of these issues prevents your use of open source tools being higher?” and the results are summarised in Table 3. Note that of the 37 respondents who mentioned the lack of tool validation, 29.7% (n = 11) of them were from the UK (totalling 52.4% of UK respondents), perhaps resulting from the need for ISO 17025 accreditation within digital forensic labs (explicitly mentioned by one respondent).

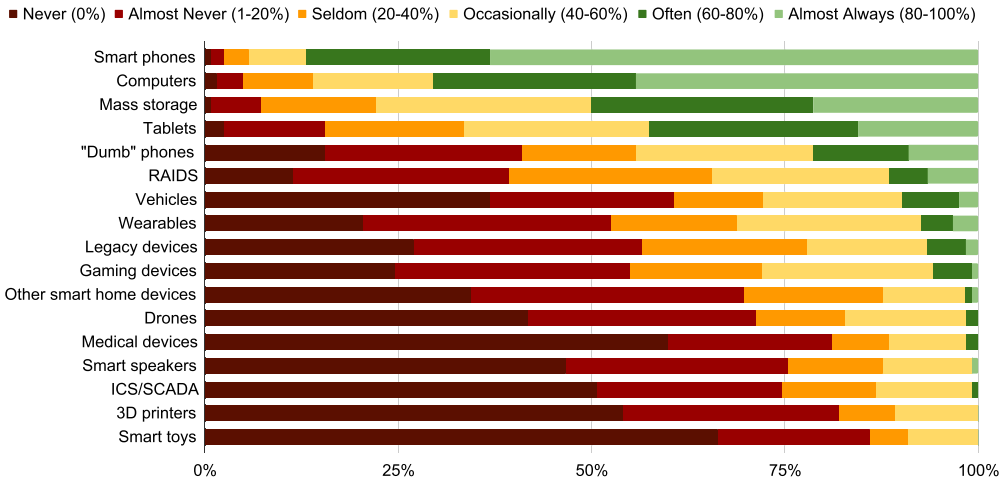


**Fig. 5.** The frequency each device type is encountered in digital investigations.

**Table 3**
Which, if any, of these issues prevent your use of open source tools being higher?

| Response | n | % |
|---|---|---|
| Functionality already available in commercial tools | 62 | 50.8 |
| Lack of time to learn a new tool | 44 | 36.1 |
| Lack of tool support (e.g. customer service) | 42 | 34.4 |
| Lack of tool validation | 37 | 30.3 |
| Lack of tool documentation | 37 | 30.3 |
| Poor compatibility with workflow | 35 | 28.7 |
| Internal policy | 35 | 28.7 |
| Unsuitable user interface | 31 | 25.4 |
| Others | 15 | 12.3 |
| None of these | 10 | 8.2 |

**Table 4**
Barriers to the use of open source tools (thematically grouped free text responses).

| Free Text Response Theme | n | % |
|---|---|---|
| Quality: Features and functionality | 4 | 26.7 |
| Quality: Overall performance | 2 | 13.3 |
| Quality: Compatibility with workflow | 1 | 6.7 |
| Quality: Number of tools | 1 | 6.7 |
| Quality: Up-to-date | 1 | 6.7 |
| Views of others: acceptance | 3 | 20.0 |
| Views of others: standards | 1 | 6.7 |
| Others | 2 | 13.3 |

There were also 15 free text responses to this question (indicated as others in Table 3), which, when categorised, contained some overlap with the closed-ended responses and are provided in Table 4.

In summary, the main barrier does appear to be that the functionality is already available in existing tools, suggesting that the perception is that open source tools are replicating functionality that is already available commercially.

The lack of time to learn a new tool is also a challenge which, if combined with the viewpoint that the functionality already exists in commercial tools, does suggest that open source tools will only be adopted if there is a need, either a capability not provided in commercial tools, or resource constraints regarding availability of commercial tools.

The lack of support, e.g. customer service or technical support, is an interesting response and likely reflects the nature of many, but not all, open source projects. Autopsy from BasisTech, for example, provides a support forum and training[1] as does Volatility,[2] but smaller projects often do not have the resources to offer training packages and rely on issue trackers within code repositories or personal contact with the tool author(s) for support. In addition, not all tools may need training, e.g. a simple hashing tool.

Lack of documentation and validation are important and actionable points for the community, and while many more mature and active open source projects, such as ALEAPP[3] and iLEAPP,[4] have up-to-date and well-written documentation, many do not.

Poor compatibility with existing workflows is also an interesting point, but requires further exploration beyond the information captured in this survey to understand and rectify. Similarly, internal policy barriers need further work to understand them and determine if they can be overcome.

Finally, unsuitable user interfaces are mentioned as an issue, but not one of the most significant, suggesting that command-line interfaces or rudimentary GUIs may not be a significant barrier to use.

## 6. Results: challenges and research directions

This section covers responses of the second part of the survey and discusses technologies that are encountered, which techniques are most used by practitioners, and other issues such as backlogs, validation, and organisational issues. It also asks an open question about what practitioners think academics should research that would most help with their work.

### 6.1. Encountered devices

Participants were asked about the different devices encountered during the investigations. The results are summarised in Fig. 5, and show that when the sum of the responses *almost always* and *often* is computed, unsurprisingly, smartphones were encountered the most frequently at 86.9% (n = 106, median = 5, IQR = 1.0), and computers 70.5% (n = 86, median = 4, IQR = 2.0). Mass storage (median = 3.5, IQR = 1.0) and tablets (median = 3.0, IQR = 2.0) were usually encountered *occasionally* or *often* (n = 69, 56.6% and n = 62, 50.8% respectively). When asked in free text for any other devices that were challenging, the following devices were also suggested that were not in the closed-ended options: backup tapes, Chromebooks, cloud, networking devices, CCTV systems, Point-of-Sale (PoS) systems, routers, tracking devices, and hardware/crypto wallets.

[1] https://www.autopsy.com/training/.
[2] https://volatilityfoundation.org/volatility-training/.
[3] https://github.com/abrignoni/ALEAPP.
[4] https://github.com/abrignoni/iLEAPP.

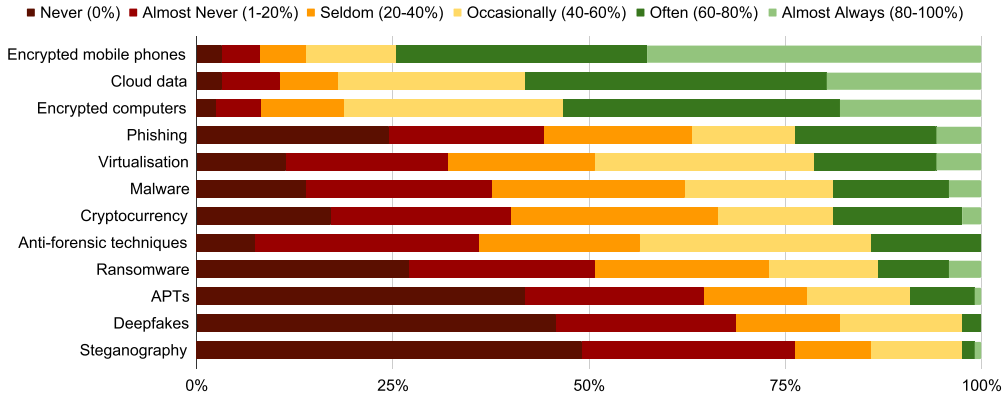


**Fig. 6.** The frequency each technology is encountered in digital investigations.

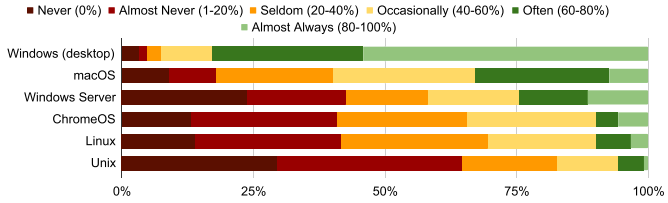


**Fig. 7.** Frequency of encountering desktop operating systems.

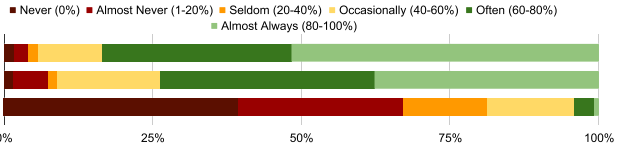


**Fig. 8.** Frequency of encountering mobile operating systems.


**Fig. 9.** Shows the frequency with which specific file systems are encountered in digital investigations.

### 6.2. Encountered technologies

In addition to devices, participants were asked how often they encountered specific technologies. The results are shown in Fig. 6.

The most common technology reported was encrypted mobile phones, with 74.6% (n = 91) responding *often* or *almost always*. Cloud data and encrypted computers were also high, with 58.2% (n = 71) and 53.2% (n = 65) respectively. Deep fakes, Advanced Persistent Threats (APTs), and steganography were very rarely encountered, with 64.6% (n = 84), 68.9% (n = 79) and 76.2% (n = 93) reporting either *never* or *almost never*. However, deepfake technology has developed significantly in recent years, so this number may become unrepresentative quickly.

### 6.3. Encountered operating systems

Participants were asked "How often do you encounter the following operating systems for analysis?". In terms of those that reported *almost always* or *often*, the most frequently encountered operating system was Microsoft Windows (n = 101, 82.6%); macOS was mainly *occasionally* or *often* (n = 64, 52.4%). ChromeOS was equally split between *almost never*, *seldom*, and *occasionally* and whilst the most frequent response for Windows Server was *never* (n = 29, 23.6%), responses are roughly equally divided between the other categories. Linux and Unix were rarely encountered, as shown in Fig. 7. Windows Server, ChromeOS and Linux all have approximately the same number of respondents (n = 52, 42.7%; n = 50, 41.0%; n = 51 41.8%) that report seeing those operating systems either *never* or *almost never*.

In terms of operating systems encountered on mobile devices, both iOS and Android were frequently encountered (n = 102, 83.6% and n = 90, 73.8% respectively, as depicted in Fig. 8.

Several additional operating systems were mentioned in the free text responses that had not been provided as options: BSD, Embedded BSD, Brew (assumed to be Binary Runtime Environment for Wireless), ColorOS, Graphine, Tails, and Windows Phone.

### 6.4. Encountered file systems

Participants were also asked about the file systems encountered, as shown in Fig. 9. The most common file system encountered is NTFS (n = 102, 83.6% selecting *often* or *almost always*), which is unsurprising given the desktop operating system results shown above. Other file systems including exFAT (n = 51, 41.8%), APFS (n = 47, 38.5%), FAT (n = 40, 32.8%), HFS(+)(n = 27, 22.1%), and EXT (n = 25, 20.5%) were also well represented as *almost always* or *often*. The free text responses here included only DHFS and proprietary formats on Digital Video Recorders (DVRs).

### 6.5. Device sources

Participants were asked where data were obtained to carry out their investigations. The results are shown in Fig. 10 and show that the data from the suspect's devices is overwhelmingly relied upon, with a majority of respondents (n = 111, 91.0%) indicating they use this source *almost always* or *often*. The second most relied-upon source was the com-

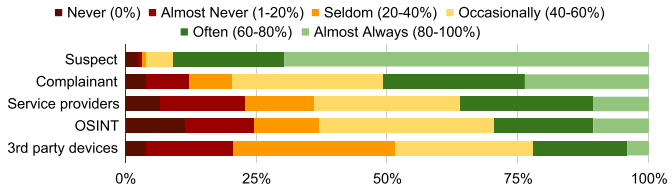


**Fig. 10.** The frequency with which particular sources of digital evidence are used in digital investigations.

plainant's device(s) (n = 62, 50.8%). Service providers and OSINT are occasionally used, and third-party devices are used the least often.

### 6.6. Use of digital forensic techniques

The participants were then asked "How often do you use the following digital investigation techniques in your work?". The results are shown in Fig. 11. The top five techniques are: keyword searching (n = 105, 86.1%, median = 5.0, IQR = 1.0), timeline analysis (n = 98, 80.3%, median = 4.0, IQR = 1.0), hashing (n = 91, 74.6%, median = 5.0, IQR = 2.0), deleted data recovery (n = 86, 70.5%, median = 4.0, IQR = 2.0), and gaining access to encrypted evidence (n = 74, 60.6%, median = 4.0, IQR = 2.0).

### 6.7. Organisational challenges

In terms of exploring non-technical challenges faced by practitioners, participants were provided with a list of potential organisational challenges and asked what impact they had on their work. The results are summarised in Fig. 12. The results indicate that high workload and insufficient staffing are the most critical challenges, along with low budget, all of which had more than 50% of respondents stating they were either *impactful* or *very impactful* (69.6% n = 85, 58.2% n = 71, and 51.7% n = 63 respectively).

Aside from the closed-ended responses from the 122 respondents, 46 responded to the free text question "Are there any other issues we should be aware of", and after filtering 'no', 'n/a' and similar responses, 27 responses remained. Two further responses were omitted from the analysis as their meaning was unclear. Of the 25 remaining responses, six referred to administrative/management factors as creating obstacles. Specifically, three respondents referred to a lack of knowledge within management, two referred to weak processes within management, and one referred to weak leadership. Five respondents referred to tools as being an issue; specifically, their cost (2 responses), time taken to procure them, lack of user knowledge, and lack of features within them. Three respondents referred to accreditation as an issue, and four answered that regulation was an issue, both in the sense that it constrains action (3) and that it causes wrong actions to be taken (1). The workload, specifically the time taken to perform the analysis, was mentioned by three people. Personnel was an issue reported by two respondents; one in reference to lack of peer support and one in relation to lack of experienced personnel. The final two responses referred to the lack of suspect cooperation and threats from perpetrators as issues. A summary of the results is shown in Table 5.

### 6.8. Backlog

Participants were asked to provide an estimate of the length of their backlogs, as shown in Table 6. In general, most of the respondents had a backlog between 0 and 3 months (30.3%, n = 37), with the same number having no backlog. However, 22.9% (n = 28) had a backlog of more than 6 months, with one reporting over 4 years. Table 6 also shows results for law enforcement only, which, compared to the overall results, show fewer people reporting no backlog. Law enforcement respondents reported a significantly higher backlog, as shown by chi-squared analysis, ($X^2(8, 117) = 17.5, p < 0.05$)). These discrepancies are not surprising given that law enforcement labs are almost certainly not in control of the number of cases that require consideration, whereas consultants, for example, can decline work if they are too busy, preventing a substantial backlog from developing in the first instance.

**Table 5**
Other organisational challenges reported.

| Theme of response | count |
|---|---|
| Administration: lack of knowledge | 3 |
| Administration: weak processes | 2 |
| Administration: weak leadership | 1 |
| Tools: cost | 2 |
| Tools: procurement | 1 |
| Tools: user knowledge | 1 |
| Tools: features | 1 |
| Regulation | 4 |
| Accreditation | 3 |
| Workload | 3 |
| Personnel | 2 |
| Other | 2 |

**Table 6**
Estimated backlog for respondents' digital forensic laboratories.

| Backlog | All (%) | LE only (%) | non-LE (%) |
|---|---|---|---|
| No backlog | 30.3 | 18.7 | 48.9 |
| 0-3 Months | 30.3 | 29.3 | 31.9 |
| 3-6 Months | 12.3 | 16.0 | 6.4 |
| 6-12 Months | 11.5 | 16.0 | 4.3 |
| 12-18 Months | 6.6 | 8.0 | 4.3 |
| 18-24 Months | 1.6 | 1.3 | 2.1 |
| Over 2 Years | 3.2 | 5.3 | 0 |
| Prefer not to say | 4.1 | 5.3 | 2.1 |

Participants were asked what factors contributed to this backlog and discounting the 30.3% who reported no backlog, the top three contributors to the backlog are the number of cases and the volume of data per case (both 54.9%, n = 67) followed by the number of devices per case (50.0%, n = 61). These are followed at some distance by inadequate triage/prioritisation policies (14.8% n = 18), delays in third-party data collection, e.g. from service providers; 13.1%, n = 16), inadequate triage/prioritisation tools (11.5%, n = 14), and delays in cross-border data collection (2.5%, n = 3). Through the 'other' option, participants added lack of staff, administrative work, quality procedures, or inadequate management.

### 6.9. Case prioritisation

Following the questions about the backlog, participants were asked whether any case prioritisation strategies were in place. The results showed that 73.8% (n = 90) replied with yes and 22.1% (n = 27) with no. The rest preferred not to answer this question.

When asked to provide further information on their top 3 highest priority case types, there were 51 responses, often indicating multiple prioritisation factors. The most common response (either standalone or with another factor) was prioritisation by the type of crime being investigated (35 respondents referred to this factor), usually listing the specific types of crime that were prioritised. For most of the respondents, this was a mixture of violent crimes, serious sexual offences, and crimes against children. Crimes against children were also given as a single prioritisation factor, for instance: "CSAM: I have been told to ignore other discovered crimes and just focus on CSAM because that's what our focus is supposed to be." In other responses, fraud and organised crime cases were referred to as prioritised.

The type of organisation for which the respondent worked is likely to have a large impact on the prioritising factor, which was referred to specifically by one respondent who made a distinction between whom the work was being done for: "In government work: Crimes against persons vs. property crimes, speedy trial, and discovery timelines. In private

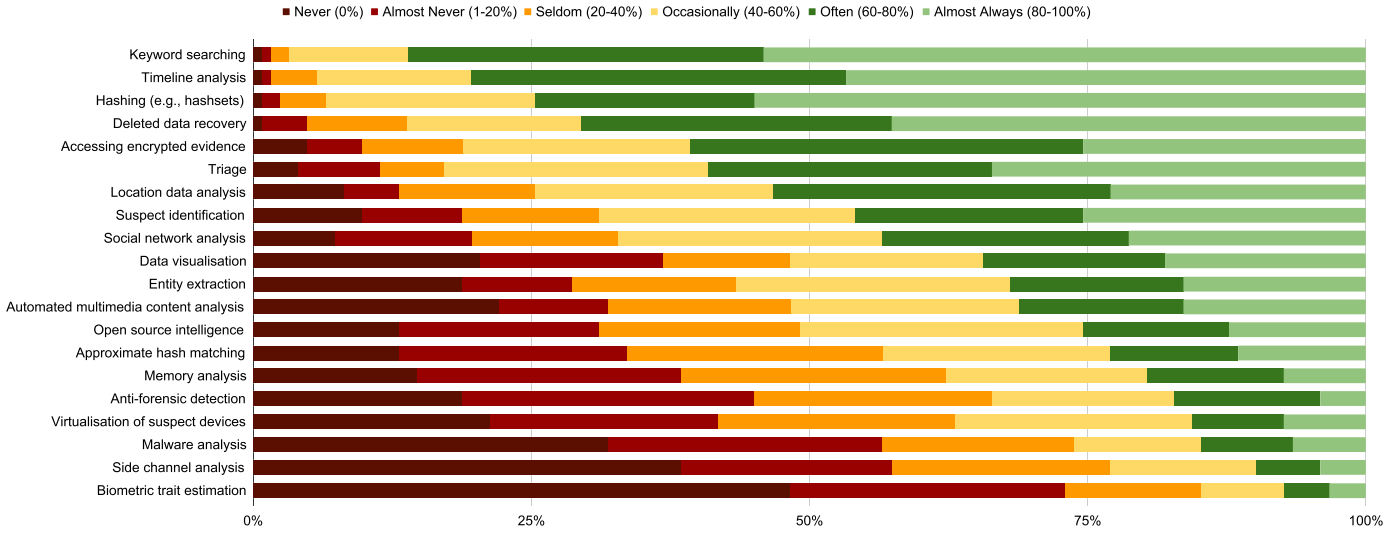


**Fig. 11.** The frequency with which specific digital forensic techniques are used. Results are sorted by the sum of *almost always* and *often* to capture the two options that describe frequent use.

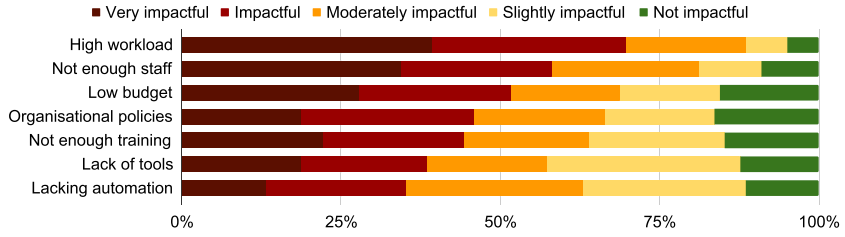


**Fig. 12.** The responses for the impact of organisational challenges on participants' work.

**Table 7**
Results for closed-ended options for "How do you validate the results of your digital forensics tools?".

| Response | n | % |
|---|---|---|
| Low-level manual validation of individual results in a case | 62 | 50.8 |
| Structured internal validation/testing programme | 54 | 44.3 |
| Rely on vendor tool testing/validation | 48 | 39.3 |
| Rely on national tool testing/validation | 43 | 35.2 |
| Rely on international tool testing/validation | 22 | 18.0 |
| Validation not considered | 8 | 6.6 |

sector work, statutory requirements regarding the reporting of suspected security incidents or complying with discovery timelines." As this quote also indicates, time was another factor, with five respondents referring to the proximity/speediness of the trial/case conclusion as a prioritisation factor. Three respondents stated that law enforcement/prosecutor decisions set priorities; cross-checking their answers to other questions in the survey indicated that two of these respondents worked on government cases and the third on industry CERT/incident response. Four respondents, who all also indicated they worked privately/in industry, referred to prioritisation by customer needs/expectations, including whether it was a new customer. Other factors referred to related to other details of the case, such as its impact, for instance, the potential to preserve life, and the volume of data involved.

### 6.10. Validation

The survey also asked: "How do you validate the results of your digital forensics tools?". The results of the closed options are shown in Table 7.

The most common response was to perform low-level manual validation of individual results in a case, and the four types of approaches based on testing/validation received responses between 44.3% and 18.0%. Only 6.6% responded that validation of results was not considered.

There were also many other values supplied within the 'other' option, and those were further examined. These were challenging to thematically group, but four responded with dual tool verification, two responded with peer review, and others were duplicates of some closed-ended responses with subtlety different wording for manual validation (n = 2), and structured internal validation testing (n = 2). The themes of the other responses could not be determined. Furthermore, one respondent highlighted the difference between validation and verification, implying that the question should have been asked about validating methods and verifying results, which is discussed further in Section 9.

### 6.11. Future research directions

Practitioners were also asked what research would be useful to them; specifically, a free text question was included: "In general, what would you like to be researched by the academic community that would most help you in your investigations?". There were 77 responses, and after removing 5 null responses, 72 remained. These were examined and thematically grouped in which responses could be added to multiple themes; therefore, the total count in Table 8 exceeds 72.

A detailed discussion of the responses is provided in the following sections.

#### 6.11.1. Research directions: artificial intelligence

Within the responses, 15 mentioned Artificial Intelligence (AI), 13 of which clearly refer to the use of AI to assist with investigations, and one mentioned forensics of AI (specifically deepfake detection). This

**Table 8**
Summary of thematically grouped responses regarding what practitioners stated the academic community should research to best help with investigations.

| Text Response Theme | n |
|---|---|
| AI | 15 |
| Artefact research | 15 |
| Bypassing encryption | 11 |
| New techniques for analysis | 8 |
| Fundamental concepts/definitions | 5 |
| Automation | 4 |
| Strategy | 4 |
| Triage | 4 |
| Cloud | 3 |
| Prioritisation | 2 |
| OSINT | 2 |

**Table 9**
Summary of uses of AI currently within digital investigations.

| Free text response theme | n |
|---|---|
| Not using AI | 17 |
| In development | 2 |
| Media categorisation | 25 |
| Coding or SQL queries | 6 |
| Content categorisation | 5 |
| Reporting | 4 |
| Unspecified filtering or analysis | 4 |
| Translation | 2 |
| Speech to text | 2 |
| OSINT | 1 |
| Triage | 1 |
| Product specific | 7 |

is discussed further in Section 6.12, but specific comments included: the impact of AI on reliability, use of AI without sharing data, content recognition, which Large Language Models (LLMs) to use, but most were non-specific and were interested in research into what AI could be used for as part of a digital investigation.

*6.11.2. Research directions: artefact research*

Artefact research was suggested in 15 responses. This theme was then expanded by adding further responses for cloud (3), drones (1), IoT (1) and vehicles (1). Within this broader category, many commented about artefacts research in general being needed, but specifics included: Windows 11, research on data retention within mobile logs, Amcache, Office 365, leveldb, and web apps (each mentioned by one respondent). Some responses highlighted that the commercial tool analysis is not complete or that the artefacts are not interpreted correctly. Others had more general ideas about the artefact-related contributions that could be made. For instance, build a framework to host parsers for lesser-used apps, as the commercial tool providers focus on big tech apps. Another suggested a need for better open source documentation of mobile databases and artefacts. Another highlighted the need for both old and new artefact research and validation.

*6.11.3. Research directions: encryption*

Research into bypassing encryption was mentioned in 11 responses, with nine suggesting device access, four suggesting encryption used by applications needed consideration (some suggested both, and in some it was not clear which), and two mentioned mobile device encryption. One response explicitly mentioned password cracking. The details here were less explicit, but it is clear that encryption of devices and applications remains a challenge, especially as encrypted mobile phones and encrypted computers are the main technologies encountered by investigators, as covered in Section 6.2.

*6.11.4. Research directions: new techniques for analysis*

Eight respondents mentioned this topic. Some specific directions were mentioned: automated link analysis and big data-driven analysis. Many of these responses focused on processing large amounts of data quickly and helping to prioritise the number of devices encountered, and a subset of these was also included in the triage and prioritisation-specific counts later.

*6.11.5. Research directions: fundamental concepts and definitions*

Five participants mentioned this topic and included differences between digital forensics and incident response, retrospective analysis of completed cases, formal reasoning, open standards, and an examination of frameworks to obtain evidence (linked to the law). There were also some comments provided that may be categorised as 'strategy'. For example, how to create "a national joined-up approach from crime scene to court related to DF practices", and a comment "We need a single repository for forensic information. Too much info is spread amongst blogs, social media posts, etc.", and from a respondent working in the "Industry CERT/Incident Response" sector, investigating digital forensics with regard to business operations and whether it reduces costs, and how it links with cyber insurance.

*6.11.6. Research directions: other topics*

The other topics that were suggested by one or two participants included: OSINT, drones, improved acquisition, vehicles, victim identification, anti-forensic technology, IoT, media, organisational research, and reliability/correctness of results. Four participants also commented on teaching-related improvements that could be made, mostly focusing on ensuring students had the necessary skills, and one on making material available in languages other than English.

*6.12. Existing and future use of AI*

Participants were asked about current uses of AI and where they thought AI could help in future investigations.

The total responses were 64, and many respondents reported that they were not using AI (n = 17), with two responding that AI use was in development. In terms of current use, the results are summarised in Table 9. The most frequent use was for the categorisation of media and content. A low number of respondents mentioned using AI for other tasks, including coding or SQL queries, reporting, or unspecified filtering, or analysis. Others mentioned translation or speech-to-text. Finally, some respondents mentioned that their use of AI was determined by the availability of AI in commercial products (n = 7), which is shown separately in the table, but overlapped almost exclusively with the categorisation of media.

In total, 76 respondents wrote a response to the free text question "Where do you think artificial intelligence could help in your future investigations?" (summarised in Table 10). Two respondents said that they did not know/were uncertain where AI could help their investigations in the future, and one said that the place for AI is still unknown. One gave an unclear response, one answered "no" and one expressed resistance to AI stating "I prefer human intelligence". Three other respondents stated that improvements in accuracy and/or explainability are needed before AI can be relied on. For example: "Bottom line is someone will need to validate the conclusions and explain how the tool came to the conclusion, whether it be to internal stakeholders or during legal proceedings."

In total, 70 respondents offered suggestions. Four of those responded in general terms, i.e. 'many' or 'major improvement'. The remaining 64 referred to particular tasks/activities that AI would assist with. Unsurprisingly, the vast majority mentioned an increase in task or tool efficiency, for instance, in the automation of tasks, the capacity for AI to reduce or collate data, and the potential for AI to assist with the production of reports. Specific tasks/activities (with respondents often referring to more than one) referred to included: image/media recognition/clas-

**Table 10**
Summary of future uses of AI in digital investigations from 76 responses. Respondents may have flagged multiple uses – as a result, totals will not equal 76.

| Free text response theme | n |
|---|---|
| Image/media classification | 12 |
| Triage | 10 |
| Searching | 9 |
| Task automation | 8 |
| Link analysis | 5 |
| CSAM | 4 |
| Summarising | 4 |
| Reporting | 3 |
| Categorisation of artefacts | 3 |
| Timelines | 3 |
| Parsing support | 3 |
| Custom scripting | 2 |
| Sentiment analysis | 2 |
| Translation | 2 |
| Face recognition | 1 |
| Prediction | 1 |
| OSINT | 1 |
| Research | 1 |
| Anomaly detection | 1 |
| Deep fake detection | 1 |
| Carving | 1 |
| Network analysis | 1 |

**Table 11**
Existing collaborations with academia.

| Response | n | % |
|---|---|---|
| Gave one or more guest lectures at a university | 36 | 37.5 |
| Taught one or more courses at a university | 28 | 29.2 |
| Provided advice with research direction/ideas | 27 | 28.1 |
| Worked on a collaborative research project with academia | 26 | 27.1 |
| Completed a dissertation as a student | 19 | 19.8 |
| Received assistance with a case from an academic / institution | 13 | 13.5 |

sification (12 responses), triage (10), searching (9), summarisation (5), link analysis (5), reporting (3), categorisation of artefacts (3), constructing timelines (3), parsing support (3). Four responses also referred to the potential for AI to assist with organisational/workplace matters. Two referred to the ability of AI to reduce exposure to CSAM, and other concepts such as sentiment analysis or deep fake detection. The other two were positive about the potential for AI, but gave a note of caution. One referred to the value of AI in supplementing, not replacing, human analysts, and the other stated: "This can't be answered in a single line because you also have to take the legit concerns of using AI in LE into consideration. AI could be helpful in creating a more efficient, responsive and effective LE model. Analysing a vast amount of data is already a challenge and will be even more in the nearby future".

## 7. Results: practitioner and academic links

The third part of the survey focused on how academic research could be better communicated to practitioners.

### 7.1. Existing collaboration with academia

First, participants were asked whether they had ever collaborated with academia and, if so, in what ways. Approximately one-third (34.4%, n = 33) responded that they had never participated in such collaborations. The remaining participants indicated involvement in various teaching or research activities or received academic support. Specifically, the responses (with multiple selections possible) are shown in Table 11.

The free text responses to this question included seven additional activities such as: currently working or having worked in academia, creating a degree programme, sponsoring internships for students, being a student, or engaging/performing research.

Participation in guest lectures and course teaching suggests that practitioners are sometimes asked to share their real-world experience and expertise with students, enriching the academic curriculum with practical insights. Providing advice on research directions or ideas and working on collaborative research projects demonstrate the potential bidirectional flow of knowledge and innovation between industry and academia. There are instances where practitioners contribute to shaping research agendas and benefit from the latest academic findings and methodologies, but the numbers are low.

For those who have collaborated with academia, the survey also enquired about the number of such collaborations over the past five years. Among 44 respondents, the median number of collaborations was three (IQR = 3). This suggests a steady level of engagement between practitioners that do have links already and academia, but no information was recorded about the depth or length of these collaborations.

### 7.2. Value of collaboration and other comments

The third question asked participants how valuable they believe the collaboration with academia is, on a scale from 0 (no value) to 5 (essential). The vast majority of participants believe it is valuable (5: 37.5% n = 36, 4: 41.7% n = 40, median = 4.0, IQR = 1.0) and no one believed that there is no value. The remaining options 3, 2, and 1 received 11, 6, and 3 responses, respectively.

The last question was an open-ended question asking for comments on collaboration with academia, which provided 35 responses. However, seven were removed from the analysis because they were yes/no responses or their meaning was unclear.

Of the 28 remaining responses, 19 were broadly positive about links with academia, either in its current or potential form. Three of these responses referred directly to existing contact with academia, for instance: "I've noticed that there was a significant increase in the relevancy of solutions offered by academia when we took them on the field with us, even for a small amount of time." Seven referred directly to a preference for more links or new kinds of links with academia, for instance: "should be embraced more" or "collaboration can focus on specific project needs and develop a symbiotic partnership, as well as promote an interest in the field for the next generation." The remaining responses were positive about links with academia in general terms or stated how the respondent found them (potentially) personally useful.

In addition, there were five negative responses. One referred to "insufficient budget" as a barrier to collaboration, and four made negative observations about academia itself. One response referred to academia as a "closed loop" that can be difficult for others to participate in, and the others referred to differences between academia and the field or the real world. For example: "Many current academic instructors have spent little time in the field, without practical experience to provide to students" and "In my opinion, a lot of academia does not reflect usage in the real world."

The remaining three responses were neutral. One referred to the need for "real work practitioners" to be involved, and another to the need to ensure that academic networks are secure before collaboration can take place. One response picked up the issue of the difference between academia and work in the field: "It is often hit or miss, depending on the faculty involved. Too many in academia have zero to no actual practical digital forensic experience."

### 7.3. Accessing academic output

To understand how practitioners acquire new knowledge, they were asked from where they obtain information. The results are summarised in Fig. 13, sorted by the sum of positive sentiment (*likely* and *very likely*) and in the case of them being equal, then by a weighted sum towards the *very likely* response.

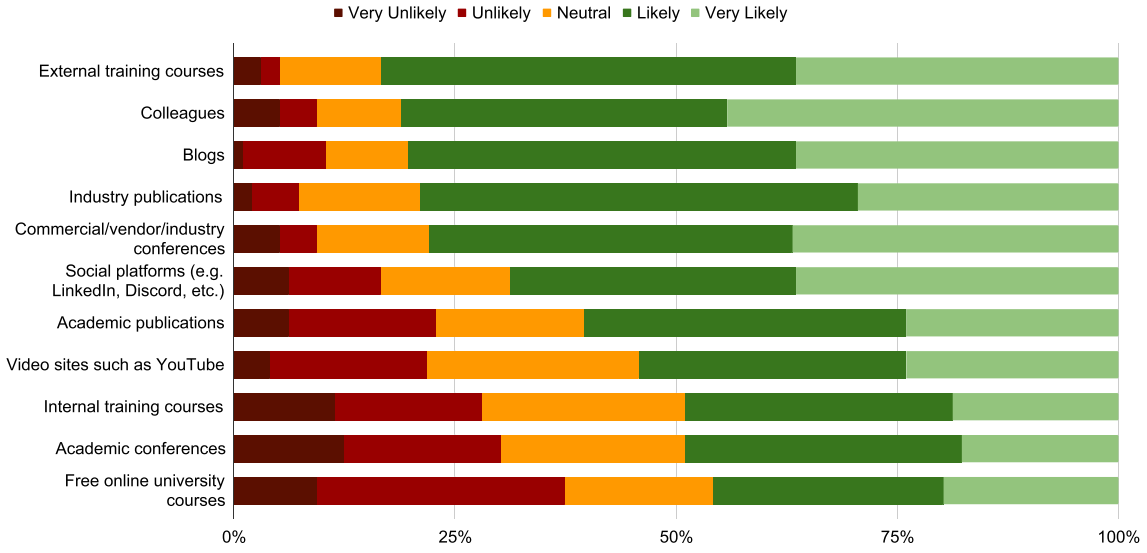


**Fig. 13.** The likelihood of obtaining information on recent digital forensic developments from different sources.

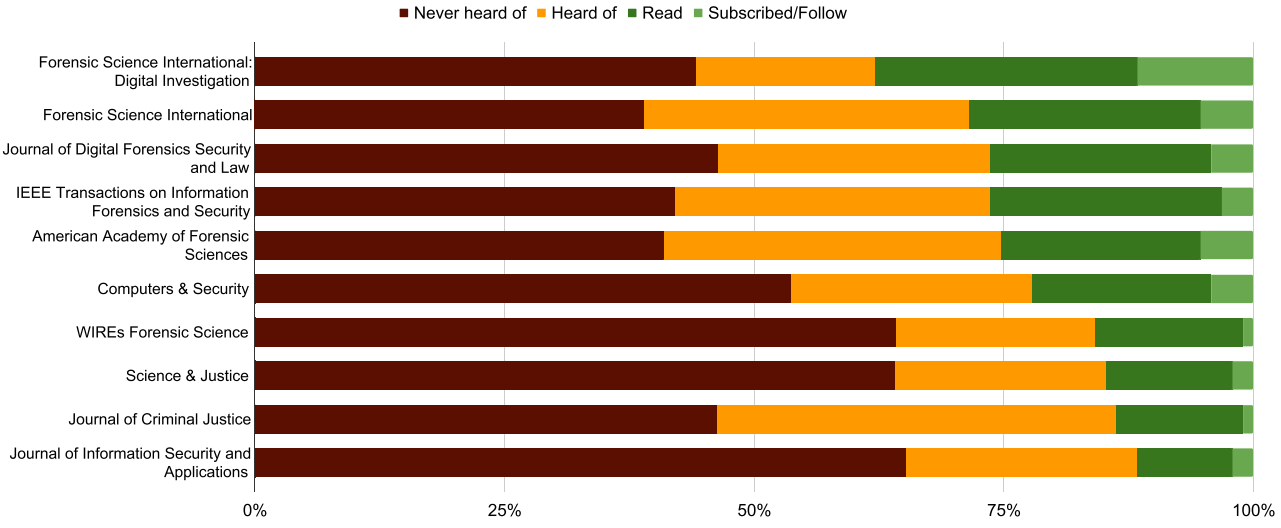


**Fig. 14.** Familiarity with specific academic journals. Sorted by sum of some level of interaction (Subscribed/Follow + Read).

The first group of popular sources of information, which contained greater than 75% (n = 72) positive sentiment, are: external training courses (83.4%, n = 80), colleagues, blogs (both 80.3%, n = 77), industry publications (78.2%, n = 75), and commercial/vendor/industry courses (77.1%, n = 74). Academic publications came seventh in the list, after social networks such as LinkedIn. Academic conferences were tenth, with only free university courses less likely to be used.

### 7.3.1. Awareness of academic journals

Participants were asked if they had heard of any from a set of established journals that commonly publish digital forensic research articles. The list of journals and responses are shown in Fig. 14. Participants could use the following responses: Never heard of, heard of, read and subscribed/follow, and the figure is sorted in descending order of some 'interaction' encapsulating the responses *read* and *subscribed/follow*. Some participants selected more than one response for each journal, so in cleaning up the data, the highest level of interaction was kept, e.g. if both *read* and *subscribed* were selected, *subscribed* was retained.

Most of the participants were unfamiliar with most journals, that is, for each journal, *never heard of* had most responses. However, Forensic Science International: Digital Investigation was the most popular with 11 (11.5%) answers for *subscribed/follow* and 26 (n = 27.1%) for *read*, followed by Forensic Science International (5.2%, n = 5 subscribed, 24.0%, n = 23 read), Journal of Digital Forensics, Security and Law (4.2%, n = 4 subscribed, 22.9%, n = 22 read), IEEE Transactions on Information Forensics and Security (3.1%, n = 3 subscribed, 24.0%, n = 23 read) and American Academy of Forensic Sciences (5.2%, n = 5 subscribed, 20.8%, n = 20 read).

The participants then responded to barriers to reading articles in academic journals. The results are shown in Table 12 with access problems (costs or lack of institutional access) being the most common reason, followed by not being aware of them and lack of time to read. The options that follow received a smaller number of responses, but it is worth noting that to assess journal articles for the properties of real-world relevance and appropriate language, access is needed, which has been highlighted as an issue.

In general, these results highlight the need to first make academic journals more accessible and/or affordable. This process has already started, with more and more institutions and funding agencies requiring open access publications (Wilkinson et al., 2016; Mombelli et al., 2024). In addition, improving communication about the availability and benefits of these journals could help bridge the gap between academic research and practical application. Better communication of 'Green' level open access would also be beneficial, whereby work published with a

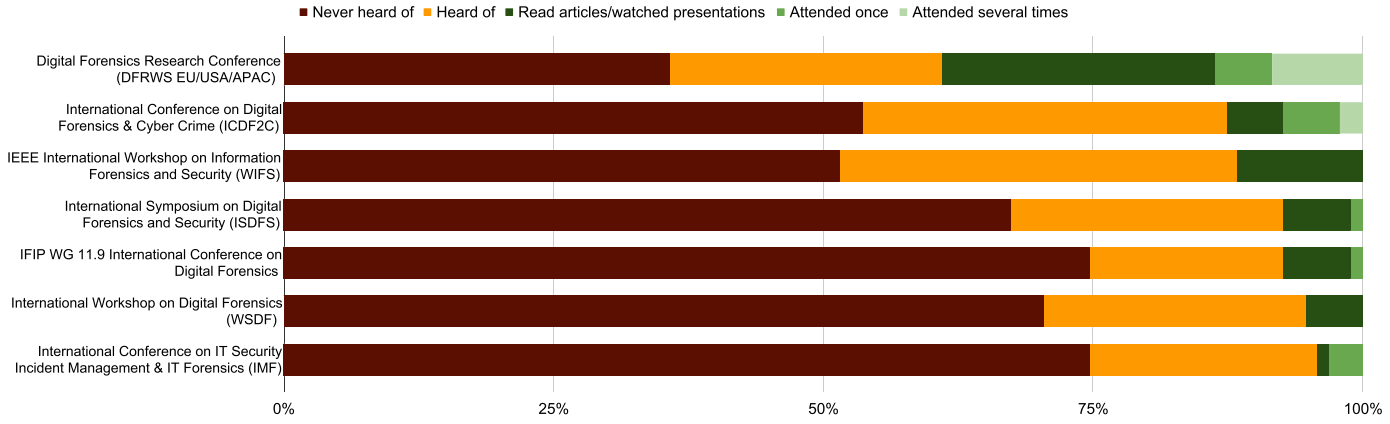


**Fig. 15.** Shows familiarity with specific academic conferences. Sorted by the sum of some level of interaction (Attended several times/Attended once/Read articles or watched presentations.

**Table 12**
Factors that are barriers to reading articles in academic journals.

| Response | n | % |
|---|---|---|
| No institutional access | 46 | 47.9 |
| Costs | 46 | 47.9 |
| I have not heard of them | 43 | 44.8 |
| Lack of time (no time given from employer) | 37 | 38.5 |
| Lack of real-world relevance | 27 | 28.1 |
| Language (academic terminology/jargon) | 7 | 7.3 |
| Language (not in preferred) | 2 | 2.1 |

**Table 13**
Desire for non-traditional formats for communicating academic research.

| Response | n | % |
|---|---|---|
| Freely available recorded talks of presentations | 78 | 81.3 |
| Podcasts | 69 | 71.9 |
| A regular consumable summary of conference or journal output, e.g. newsletter | 64 | 66.7 |
| Low cost virtual conference attendance | 58 | 60.4 |
| None | 2 | 2.1 |
| Other | 5 | 5.2 |

publisher is made available open access via the university's institutional repository.

The second tier of responses around the lack of real-world relevance and use of academic terminology is likely under-represented due to the barriers to access that were identified earlier. This also needs to be addressed. Increased cooperation and collaboration between academia and practitioners is likely to be the key to achieving improvements in this area.

#### *7.3.2. Awareness of academic conferences*

In addition to journals, participants were also asked about digital forensic academic conferences. The results are shown in Fig. 15 and are sorted by the sum of some level of interaction, read articles or watched presentations, attended once or attended several times.

As with academic journals, the never-heard-of option was most common in all venues. On the other hand, only DFRWS (n = 8, 8.3%) and ICDF2C (n = 2, 2.1%) have been attended by participants several times. In total, only 26.0% (n = 25) of respondents had attended any conference.

The reasons preventing them from attending academic conferences are similar to before: Cost (66.7%, n = 64), unaware of them (58.39%, n = 56), lack of time (no time given from employer) (42.7%, n = 41), lack of relevant content (16.7%, n = 16), language (not preferred language) (7.3%, n = 7), language (academic jargon) (3.1%, n = 3). Only 2.1% (n = 2) indicated that they have no interest in attending.

#### *7.3.3. Non-traditional formats for academic research*

Participants were asked to consider "Which, if any, of these non-traditional formats for academic research would you be interested to follow?" This was designed to solicit methods to improve the communication of research to practitioners. The results are summarised in Table 13. The most popular option of freely available recorded talks does not involve a change of format and simply requests that the conference presentation is available freely and on demand rather than at a specific time and specific location. The fourth option "low cost virtual conference attendance" also does not require a format change but does require a change in attendance module and technical resources to stream the conference content, although some conferences are already offering this, e.g. DFRWS. The remaining options: podcasts and summary newsletters of research output do require additional processing and summarisation of the content produced, but with 71.9% (n = 69) and 66.7% (n = 64) of respondents saying they would be interested in following such output, this may be worth further consideration and discussion.

## 8. Discussion

Given the results discussed in the previous sections, this section provides a discussion and reflection on what academia can learn from these practitioner responses.

### *8.1. Challenges faced by practitioners*

The survey results have shown there are different challenges faced that can be broadly categorised as technical and organisational.

The survey provided information about the devices, technologies, operating systems, and file systems encountered. However, the extent to which these encounters remain challenges was not captured. Within the research direction questions, artefact research and bypassing encryption were frequent responses that can be mapped to the technologies encountered. Although outside the scope of this paper, a mapping of technologies encountered with the academic knowledge base on those topics would be interesting to identify any discrepancies from that perspective.

It is also worth noting that the use of AI and new techniques to improve analysis was suggested to be useful to address some challenges. The survey also identified the types of techniques most often used by practitioners (keywords, timelines, hashing, etc.). Again, it was not asked if the specific techniques were sufficient, but a review of academic understanding of these areas and problems within them may be beneficial in evaluating where research effort is directed.

In terms of organisational challenges (discussed in Section 6), the most impactful were: not enough staff, high workload, and low bud-

get, but not enough training, tools, and organisational policies also had an effect. These are all difficult for the digital forensics academic community to influence, but there may be other areas of academia, e.g. organisational research, that may have outputs that could be applied. In addition, recent discussions on the use of AI offer the potential to assist in investigations, but it remains unclear exactly where to safely apply such technology Scanlon et al. (2023b,a).

### 8.2. Communication of research

Section 7 reveals that the communication of academic research to practitioners is, frankly, inadequate. Academic journals are consulted far less frequently for information compared to industry training courses, publications, vendor conferences, and even social platforms and blogs. Academic conferences do even worse in terms of engagement. Unfortunately, these findings might represent an optimistic scenario, as the survey is biased toward respondents who were already somewhat engaged, suggesting that the actual situation in the broader practitioner community may be even more concerning. The reasons for the lack of engagement can be attributed to access (cost, subscriptions, etc.), which may be addressed through open access publishing and communicating the nature of the open access.

However, it is also important to acknowledge and reflect on 28.1% of respondents suggesting that the barrier was a lack of real-world relevance, given that access problems, could be a low estimate. Although academic work is not necessarily intended to be of practical (immediate) relevance and some work contributes to establishing the theoretical basis of the field, some work is intended to be of use and is presented as such. If work in that category fails to achieve its relevance goals, then additional efforts are needed to close that gap. Greater engagement with practitioners during the publishing or review process could help improve the situation.

Conferences such as DFRWS have best paper awards based on their reviews (by predominantly academics), and perhaps a Practitioner Award could also be established to highlight papers most beneficial to the practitioner community. The lack of time was also mentioned and different delivery methods were discussed, but this is also linked to the relevance of the work. If the work is relevant, applicable, helpful, and is well communicated, then time may very well be found to engage with the content.

### 8.3. AI in digital forensics

Section 6.12 discussed the current and potential future use of AI from a practitioner's perspective. The results suggest that AI is used in a limited capacity in digital forensics, predominantly in media categorisation. However, there were suggestions for its use in other areas (discussed in Section 6.12). Although the ideas of the practitioners here are invaluable, as AI is a fast-moving area, it is difficult to predict where the most beneficial future uses will be. The concerns of practitioners, e.g. the need for accuracy, explainability, validation, and privacy, were also captured and echo those identified in the literature on the topic (Scanlon et al., 2023a,b; Michelet and Breitinger, 2024). These are useful criteria for researchers working in this area to consider.

### 8.4. Practical realisation of research output

Section 7 identified that the communication of digital forensic academic research is poor. There is also some evidence that the practitioners' use is driven by what is available in commercial tools (see AI results in Section 6.12). It has also been seen that the usage of open source tools is relatively low (Section 5.4). This presents the challenge of how to get practical research output into the hands of practitioners.

Consider two outputs from digital forensic research, artefacts and techniques, which, in the analysis of 10 years of papers from the DFRWS EU conference (Breitinger et al., 2024), represent approximately 10% and 20% of the output respectively. If there is artefact-based knowledge resulting from research, then there is a question as to how this could be directly integrated into practitioner workflows. There are options from tool vendors such as Magnet Artefact Exchange, but this is proprietary and is only available to Magnet customers. DFIR Review[5] provides a platform to publish peer-reviewed short artefact-based research articles with reviews of methodology and verification of results against user-supplied and reviewer-generated datasets, but is not able to offer direct tool integration of the published results. Open environments have been created to document forensic artefacts in machine readable format, e.g. the Artefact Genome Project (AGP) Grajeda et al. (2018) and Casey et al. (2022). The latter, including concepts such as voting mechanisms to capture the level of acceptance, would be of great benefit, but with the ability to directly import into tools used by practitioners via a standard representation, e.g. the CASE ontology.

For the second scenario in which a researcher has developed a useful technique, creation of an open source implementation is possible, but there are many barriers to using these by practitioners, as discussed earlier. Integration into the tools used by practitioners would be the most direct way to make the developed technique usable, and there are two ways that this could be achieved. The first is directly by the tool vendors, but this relies on it getting to the top of their development backlogs, which are likely driven by customer demands, which, as awareness of academic research is low, is therefore unlikely. The second is for the researcher to target a particular tool and try to integrate their technique directly, which is in some cases possible as some tools offer plugin frameworks, e.g. X-Ways X-Tensions, but most require the researcher to have access to that paid tool to undertake the development and testing needed to add capabilities to these commercial offerings.

Therefore, a practical solution to improving the technology transfer of techniques from researchers to practitioners remains a challenge. Common API access within tools, plugin-based functionality would help, but as would free access to limited versions of commercial tools to researchers, with the latter presumably making minimal impact on the vendor's bottom lines. This option would allow researchers to produce plugins for tools that are used by practitioners, extending their capabilities, but would incidentally also allow researchers to generate datasets and perform tests on specific features of these tools, e.g. Hargreaves et al. (2024b). Taking this further and adopting a model common in the security domain, a 'bug bounty' programme from forensic tool vendors, either for problems in parsing, but also overcoming limitations in functionality, would essentially crowdsource digital forensic tool testing and ultimately improve quality and capability in digital investigations.

### 8.5. Knowledge transfer

Given the amount of time in the current role and the amount of time working in digital forensics ranging from 1-40 years, there are significant differences in experience (Section 4.4). This survey did not investigate the extent to which the knowledge and experience of people who have worked for a long time in the field is transferred to those newer investigators. Determining how effectively this is performed and possibly improving this process ensures that knowledge is not lost as investigators leave the workforce, which is something that is already being researched in many other areas (Burmeister and Deller, 2016). If this is indeed an unsolved problem, it may be useful for digital forensics researchers to leverage existing results from non-digital forensic academic literature and rely on interdisciplinary work with other areas such as informational and knowledge management, and apply that to the digital forensics field.

### 8.6. Education and training

Of course, academia is not just about research, but also about education. Overall 73.8% of respondents already have some university

[5] https://dfrws.org/dfir-review/.

education, but in some cases this was awarded several years ago (median = 8.5 years, IQR = 13, see Section 4.5). With many practitioners having limited time for education and training (with 29.5% having five days available or fewer, and 10.7% having zero), this raises questions about the role of academia from a continuous education perspective. Given 46.7% reported having an MSc or equivalent, there is still some scope for further study at Master's level. However, given the lack of time available for training and the cost (in terms of finances and/or time), it is important to ensure that such courses offer tangible benefits to the employer as well as the individual. Further study at PhD level is another option, and may be appealing given it also has the option for part-time study, has a research focus, and affords some workload flexibility. However, for part-time study, this is likely a 6-8 year commitment, which is challenging, and it is not clear if this is required or desirable within digital forensic labs.

In Section 4.3, the experience of the participants was reported. Although expertise in computer forensics, mobile forensics and acquisition was relatively high, fewer practitioners reported the higher end of the expertise scale for the forensic analysis of databases, networks, memory, cloud, IoT, and other non-traditional devices, e.g. drones, vehicles, etc. Given the numbers for university education mentioned above (73.8%), this could suggest some limitations of the scope of the curriculum in terms of providing education in these newer areas. However, Sections 6.1 and 6.2 discussed the frequency with which devices and technologies were encountered, and devices that had lower levels of expertise (vehicles, drones, smart devices) were very infrequently encountered, so there may be multiple factors involved in the lower level of expertise.

Finally, the development of short, focused professional courses presents an opportunity to complement vendor-based offerings. However, these courses must deliver practical benefits comparable to those provided by existing professional, non-academic programs in this field.

To ensure that content is up-to-date and relevant, the participation of practitioners in curriculum development is likely to be highly beneficial, either directly or via the equivalent of Industrial Advisory Board (IAB) common for other disciplines. The establishment of such links may also offer other opportunities, such as sharing potential MSc research project topics.

### 8.7. Diversity

Finally, as shown in Section 4, there is an imbalance in gender in the respondents. If this is extrapolated to represent an imbalance within the practitioner community, then, as with other STEM-related subjects, there is much work to do to address this gender imbalance.

Work to improve gender balance in STEM subjects needs to be addressed earlier in the pipeline than solely in the workplace or in academia, where there is some existing effort, e.g. the Women in Forensic Computing Workshop (WinFC).[6] Academics should continue to address the low number of women in STEM, both at the university level, but also through outreach at earlier points in the education system, for which there is also some existing effort, e.g. The Cyber Sleuth Science Lab.[7]

The survey did not consider other typical diversity characteristics such as age, disability, race and ethnicity, religion and belief, sexual orientation, or other socioeconomic characteristics. Although some of those should be included in future surveys, race and ethnicity are difficult to derive any meaningful findings from in a worldwide survey unless sufficient data per country are obtained to consider appropriate representation.

[6] https://www.cybercrime.fau.de/winfc2024/.
[7] https://www.cybersleuthlab.org.

## 9. Limitations and further work

Despite a good response rate of 122 participants, the sample size remains limited. In addition, aside from the larger set of responses from the US and UK, it is difficult to say anything conclusive about differences between individual countries, although some regional grouping comparisons were made. In future, expanding the reach of the survey would provide opportunities for additional analysis.

Some limitations were also created due to the promotion strategy of the survey. Firstly, the authors were primarily responsible for the dissemination, which means through the network that the authors have there may be bias in the responses. Secondly, DFRWS EU was used as a promotion mechanism, which affects some results such as awareness of conference venues. Future surveys will need to be distributed much more widely by as diverse a group of people as possible to minimise bias in the responses.

In terms of future surveys, many refinements have been identified in reviewing the responses. The most significant omission was that participants were asked what technologies they encountered but were not specifically asked if the devices posed a challenge or were handled well with existing techniques (although some challenges were captured in the other free-text questions). This is a general theme where additional information was needed to further understand the data received, e.g. when a participant was involved in a large number of cases, the survey did not ask about the nature of the involvement. It would also have been interesting to ask about specific tooling rather than just the proportion of open source tools. This would allow researchers who wish to provide implementations that allow their work to be used by practitioners to decide if they wanted to target a particular tool or plugin framework. In addition to requesting more detailed information, there were also specific questions that need re-wording to improve precision, e.g. the validation vs. verification topic (discussed in Section 6.10), which is clarified in Marshall and Paige (2018) and this can be used to refine the question. However, all of these improvements must be balanced with ensuring that the duration of the survey remains reasonable.

Other refinements include that participants were not asked about race, age, or other characteristics relevant to a diverse workforce, which given Wagstaff and LaPorte (2018) is a probable omission. There may also be some instances of academics responding and skewing data, as discussed in Section 5.4. This is complicated to fix, as many of the respondents with 'academic' as a primary role are engaged in practitioner work but may have different perspectives and requirements to front-line policing. This has been mitigated within the survey by collecting these demographic data, and topics such as the backlog were also considered from an law enforcement perspective only to gain the most insight, i.e. those without control over incoming cases compared with those engaged in consulting. It is also important to understand more about tool usage, which may vary in different countries in terms of resources and open source usage.

Only one practitioner was consulted in the construction of this survey, which is suboptimal, and since the survey did not offer the question "Is there anything else you wish to tell us", knowledge of other insightful questions from the practitioner's perspective that could have been asked within this survey is still lacking.

In terms of the questions that were asked, from a participant perspective, some were not as straightforward to complete as they could have been, for example, the number of cases per year and lab size were provided as numeric free text, which was chosen as no information was available to estimate appropriate bracketed options, which given the results presented as part of this paper would now be possible.

However, as a result of these and similar issues and reflections, it has become apparent that any future version of this survey should be developed in conjunction with practitioners so that the most informative questions are asked, using appropriate terminology for the target participants, with appropriate options to facilitate ease of completion.

Future surveys will correct these issues identified, be able to add questions to fill in identified gaps, e.g. specific tooling, but they will also allow trends to be tracked longitudinally. A Google Form has been set up for practitioners and academics to submit feedback, suggestions, and requests for what should be included in the next iteration of the DFPulse survey.[8]

In terms of further use of the survey data, there are many examples in which the data could be cross-correlated to gain additional insight. For example, in the future directions section, one participant mentioned the differences between digital forensics and incident response; these data could be further sliced by Industry CERT/Incident Response vs. law enforcement and consider the differences in responses.

To this end, the survey response data is available online (Hargreaves et al., 2024a), with some fields removed or provided with reduced precision to reduce the risk of deanonymisation. The free text responses have been separated from the other data, the country replaced with high-level regions, the year in role and lab size placed into brackets, and the gender of the respondents removed. The release of this dataset should facilitate further analysis and gain additional insight into the digital forensic practitioner community.

## 10. Conclusions

This paper has reported on the results of an extensive survey of practitioners, including the nature of the environment in which they work, the challenges faced, and the extent to which they are involved with academia.

There are many applications of this work, including providing insights into the environments, challenges, and technologies encountered, which can provide inspiration for research direction. It can support otherwise unevidenced assertions in research, or particular techniques being important within digital forensics. The results also allow some reflection within the academic community on the research that is conducted and especially on how it is communicated. The formalisation of the field and peer review is important in cementing digital forensics as a scientific discipline, but if it does not reach the practitioner community, then it risks falling into one of the less desirable definitions of academic: "strictly theoretical or formal . . . of no consequence, irrelevant" (Oxford English Dictionary, 2024).

The need for greater collaboration between practitioners and academics is frequently discussed, and this paper highlights the need to reboot these efforts in a practical sense. The following actionable points for the academic community have been extrapolated from the results but are not exhaustive:

- Consider the practical applications of research, importantly, in collaboration with practitioners when deciding where to direct the research effort.
- Review open source efforts and work on highlighting benefits.
- Given the current reliance on commercial tool offerings, collaborations with tool vendors and the possible knowledge transfer from academia to commercial tools should be explored.
- Implement the alternative information sharing methods suggested.
- Involve practitioners in curriculum development to ensure the relevance of topics and materials.
- Repeat an enhanced version of this survey in the future to measure the success of sharing initiatives.

Despite the less than positive findings on awareness of academic work, there are encouraging results. For example, the response to the question "How valuable do you believe collaboration with academia is" results in the vast majority of participants believing that it is valuable (see Section 7.1) and none of the respondents believing that it is not valuable. This shows that the will to engage is there, but extensive work is needed to remove barriers to this engagement.

[8] https://forms.gle/yHEM42QwqdabjMm16.

## CRediT authorship contribution statement

**Christopher Hargreaves:** Writing – original draft, Methodology, Investigation, Conceptualization. **Frank Breitinger:** Writing – original draft, Investigation, Conceptualization. **Liz Dowthwaite:** Writing – review & editing, Formal analysis, Data curation. **Helena Webb:** Writing – review & editing, Formal analysis, Data curation. **Mark Scanlon:** Writing – review & editing, Methodology, Conceptualization.

## Declaration of competing interest

Frank Breitinger, Christopher Hargreaves, and Mark Scanlon are members of the organising committee for the DFRWS conference and on the editorial board for the FSI: Digital Investigation journal. Frank Breitinger and Mark Scanlon are also on the board of directors of DFRWS. References to both of these organisations are made in the article, but the results are presented in full, with the raw data from the survey responses. Otherwise, the authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this document.

## Acknowledgements

Thank you to all respondents and those who shared the survey; in particular: Jessica Hyde, Heather Charpentier, Alexis Brignoni, and Johann Polewczyk. Also thank you to Johann Polewczyk and John Sheppard for reviewing the survey before public release. Helena Webb and Liz Dowthwaite are funded by the UKRI Trustworthy Autonomous Systems Hub (EP/V00784X/1) pump prime project "Trustworthy and Useful Tools for Mobile Phone Extraction".

## Data availability

Data is available and linked in the article.

## References

Airlie, M., Robertson, J., Krosch, M.N., Brooks, E., 2021. Contemporary issues in forensic science—worldwide survey results. Forensic Sci. Int. 320, 110704. https://doi.org/10.1016/j.forsciint.2021.110704. https://www.sciencedirect.com/science/article/pii/S0379073821000244.

Al Fahdi, M., Clarke, N., Furnell, S., 2013. Challenges to digital forensics: a survey of researchers & practitioners attitudes and opinions. In: 2013 Information Security for South Africa, pp. 1–8.

Baechler, S., 2017. Do we need to know each other? Bridging the gap between the university and the professional field. Policing: J. Policy Pract. 13, 102–114. https://doi.org/10.1093/police/pax091.

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. In: DFRWS EU 2024 - Selected Papers from the 11th Annual Digital Forensics Research Conference Europe. Forensic Sci. Int. Digit. Invest. 48, 301685. https://doi.org/10.1016/j.fsidi.2023.301685. https://www.sciencedirect.com/science/article/pii/S2666281723002044.

Burmeister, A., Deller, J., 2016. Knowledge retention from older and retiring workers: what do we know, and where do we go from here?. Work Aging Retire. 2, 87–104. https://doi.org/10.1093/workar/waw002.

Casey, E., Nguyen, L., Mates, J., Lalliss, S., 2022. Crowdsourcing forensics: creating a curated catalog of digital forensic artifacts. J. Forensic Sci. 67, 1846–1857.

Forensic Capability Network UK, 2020. Digital forensic science strategy. https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/2020/national-digital-forensic-science-strategy.pdf.

Garfinkel, S., 2022. Digital forensics past and future. https://simson.net/ref/2022/2022-06-10.pdf.

Garfinkel, S.L., 2010. Digital forensics research: the next 10 years. Digit. Investig. 7, S64–S73.

Grajeda, C., Sanchez, L., Baggili, I., Clark, D., Breitinger, F., 2018. Experience constructing the artifact genome project (AGP): managing the domain's knowledge one artifact at a time. Digit. Investig. 26, S47–S58. https://doi.org/10.1016/j.diin.2018.04.021. https://www.sciencedirect.com/science/article/pii/S1742287618302007.

Gurule, K., 2016. An analysis of digital forensic units. Master's thesis. Purdue University.
Hargreaves, C., Breitinger, F., Dowthwaite, L., Webb, H., Scanlon, M., 2024a. DFPulse: the 2024 digital forensic practitioner survey (response dataset). https://doi.org/10.5281/zenodo.13612567.
Hargreaves, C., Nelson, A., Casey, E., 2024b. An abstract model for digital forensic analysis tools - a foundation for systematic error mitigation analysis. In: DFRWS EU 2024 - Selected Papers from the 11th Annual Digital Forensics Research Conference Europe. Forensic Sci. Int. Digit. Invest. 48, 301679. https://doi.org/10.1016/j.fsidi.2023.301679. https://www.sciencedirect.com/science/article/pii/S2666281723001981.
Hranickỳ, R., Breitinger, F., Ryšavỳ, O., Sheppard, J., Schaedler, F., Morgenstern, H., Malik, S., 2021. What do incident response practitioners need to know? A skillmap for the years ahead. Forensic Sci. Int. Digit. Invest. 37, 301184.
Larsen, O.H., Ngo, H.Q., Le-Khac, N.-A., 2023. A quantitative study of the law enforcement in using open source intelligence techniques through undergraduate practical training. Forensic Sci. Int. Digit. Invest. 47, 301622. https://doi.org/10.1016/j.fsidi.2023.301622. https://www.sciencedirect.com/science/article/pii/S2666281723001348.
Luciano, L., Baggili, I., Topor, M., Casey, P., Breitinger, F., 2018. Digital forensics in the next five years. In: Proceedings of the 13th International Conference on Availability, Reliability and Security ARES '18. Association for Computing Machinery, New York, NY, USA.
Marshall, A.M., Paige, R., 2018. Requirements in digital forensics method definition: observations from a UK study. Digit. Investig. 27, 23–29. https://doi.org/10.1016/j.diin.2018.09.004. https://www.sciencedirect.com/science/article/pii/S1742287618302718.
Michelet, G., Breitinger, F., 2024. ChatGPT, Llama, can you write my report? An experiment on assisted digital forensics reports written using (local) large language models. In: DFRWS EU 2024 - Selected Papers from the 11th Annual Digital Forensics Research Conference Europe. Forensic Sci. Int. Digit. Invest. 48, 301683. https://doi.org/10.1016/j.fsidi.2023.301683. https://www.sciencedirect.com/science/article/pii/S2666281723002020.
Mombelli, S., Lyle, J.R., Breitinger, F., 2024. Fairness in digital forensics datasets' metadata–and how to improve it. Forensic Sci. Int. Digit. Invest. 48, 301681.
Oxford English Dictionary, 2024. Academic, adj., sense 5. https://doi.org/10.1093/OED/9018293275.
Palmer, G., et al., 2001. A road map for digital forensic research. In: First Digital Forensic Research Workshop. Utica, New York, pp. 27–30.
RCFL, 2024. Rcfl file repository. https://www.rcfl.gov/file-repository.
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. Investig. 29, S124–S142. https://doi.org/10.1016/j.diin.2019.04.005. https://www.sciencedirect.com/science/article/pii/S1742287619301549.
Scanlon, M., Breitinger, F., Hargreaves, C., Hilgert, J.-N., Sheppard, J., 2023a. ChatGPT for digital forensic investigation: the good, the bad, and the unknown. Forensic Sci. Int. Digit. Invest. 46, 301609. https://doi.org/10.1016/j.fsidi.2023.301609. https://www.sciencedirect.com/science/article/pii/S266628172300121X.
Scanlon, M., Nikkel, B., Geradts, Z., 2023b. Digital forensic investigation in the age of ChatGPT. Forensic Sci. Int. Digit. Invest. 44, 301543. https://doi.org/10.1016/j.fsidi.2023.301543.
Seigfried-Spellar, K.C., 2018. Assessing the psychological well-being and coping mechanisms of law enforcement investigators vs. digital forensic examiners of child pornography investigations. J. Police Crim. Psychol. 33, 215–226.
Sremack, J.C., 2007. The gap between theory and practice in digital forensics. In: Annual ADFSL Conference on Digital Forensics, Security and Law, vol. 2.
Vasilaras, A., Papadoudis, N., Rizomiliotis, P., 2024. Artificial intelligence in mobile forensics: a survey of current status, a use case analysis and ai alignment objectives. Forensic Sci. Int. Digit. Invest. 49, 301737. https://doi.org/10.1016/j.fsidi.2024.301737. https://www.sciencedirect.com/science/article/pii/S2666281724000568.
Wagstaff, I.R., LaPorte, G., 2018. The importance of diversity and inclusion in the forensic sciences. NIJ J 279, 81–91.
Wilkinson, M.D., Dumontier, M., Aalbersberg, I.J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., da Silva Santos, L.B., Bourne, P.E., et al., 2016. The fair guiding principles for scientific data management and stewardship. Sci. Data 3, 1–9.