



ASSESSMENT – TASK 1

Research Report

Digital Forensic Analysis

ACCA7031

Report date: *28th of April 2026*

By: *Amélie SERVANT*

Digital Forensics: Current State, Intersection with Cybersecurity, Emerging Trends, Challenges and Job Opportunities

Current State of the Field

Digital forensics is the field concerned with the identification, preservation, analysis, and presentation of digital evidence in a way that is reliable and admissible in court. Once primarily associated with criminal investigations involving seized computers, it is now much broader. It now encompasses smartphones, cloud environments, networks, RAM, connected devices, and other connected systems. This evolution reflects the increasing reliance of organizations and individuals on digital technologies, and the concurrent rise of cybercrime, corporate fraud, insider threats, and data breaches. Recent standards and research confirm that this discipline is becoming more central, but also more complex, particularly due to distributed infrastructures, remote environments, and the increasing volume of digital evidence (NIST, 2024; DFRWS, 2024).

The current state of digital forensics reveals a field that is both diverse and highly technical. It now encompasses several subfields, such as computer forensics, mobile forensics, memory forensics, network forensics, and cloud forensics. Modern investigations are rarely limited to a single hard drive or isolated device. On the contrary, experts often have to work with multiple devices, systems, and types of artifacts within the same case. This expansion is one of the defining characteristics of the field, but it also significantly increases the complexity of investigations and the range of skills required of digital forensics analysts. In other words, the field has evolved from a highly technical practice to a multidisciplinary investigative function (DFRWS, 2024; Kävrestad, 2024).

Tools: Features and Capabilities

This evolution is also reflected in the tools commonly used in practice. Magnet AXIOM is widely used to analyze evidence from computers, mobile devices, and cloud sources within a unified case management environment. Its strength lies in cross-source correlation and automated artifact analysis. Cellebrite UFED remains the industry standard for mobile data extraction and analysis, supporting physical, logical, and file system acquisitions across a wide range of devices. Autopsy remains a relevant open-source platform for file system analysis, deleted file recovery, and event timeline reconstruction, while Volatility is a central memory forensics tool for examining running processes, loaded modules, and potential malware activity in RAM. Velociraptor, an open-source DFIR tool designed for endpoint monitoring, remote evidence collection, and large-scale incident response, is another increasingly important platform. Unlike traditional forensic tools that focus on individual devices, Velociraptor enables rapid triage across

hundreds of terminals simultaneously, making it particularly valuable in enterprise environments (Velociraptor, 2025; Magnet Forensics, 2025; Cellebrite, 2025).

However, simply listing these tools without critically evaluating them is insufficient. No single platform covers the entirety of the forensic context, and the choice of tool has direct consequences for the reliability and admissibility of evidence. Commercial tools are generally powerful and well-integrated, but their internal processes are often opaque, which can raise questions about reproducibility in a legal context. Open-source tools offer greater flexibility and transparency but generally require more expertise and time from the analyst. Therefore, the choice of tool is not only a technical decision but also a strategic one. In practice, the reliability of investigations relies on combining several tools and validating the results rather than on a single platform, particularly when evidence may be challenged later in court, during disciplinary proceedings, or regulatory investigations (Kävrestad, 2024).

Intersection of Digital Forensics and Cybersecurity

Digital forensics is closely linked to cybersecurity. Cybersecurity aims to prevent, detect, and contain threats, while digital forensics provides the analytical tools needed to understand what happened, how, which elements were affected, and what evidence to preserve. In practice, these two fields are increasingly converging thanks to Digital Forensics and Incident Response (DFIR). According to the Magnet Forensics State of Enterprise DFIR (2025) report, forensic analysis is now frequently integrated into incident response processes, endpoint triage, and post-breach investigations. This development is significant because it demonstrates that digital forensics is no longer purely reactive. It is now an integral part of operational cybersecurity, particularly in ransomware investigations, insider threat cases, malware analysis, and data breach notification.

At the same time, this close collaboration creates operational tensions. Cybersecurity teams generally prioritize speed, containment, and system recovery, while forensic analysis demands methodological rigor, comprehensive documentation, and the integrity of evidence. These priorities do not always align during an ongoing incident. For example, quickly isolating a compromised system is a good security practice but can destroy volatile data or break the chain of custody. This tension partly explains why forensic preparedness is increasingly considered a core component of cybersecurity maturity frameworks, rather than a secondary consideration (NIST, 2024).

Emerging Trends in Digital Forensics

Several emerging trends are shaping the future of the discipline. One of the most structurally significant is cloud forensics. NIST Special Publication 800-201 (2024) proposes a reference architecture for cloud forensics, demonstrating that cloud environments require fundamentally different forensic approaches. Unlike local device analysis, evidence from the cloud can be distributed across multiple geographic regions, be partly volatile, and partly controlled by third-party service providers whose

cooperation may be limited or delayed. This creates technical challenges, such as acquiring evidence without physical access to hardware, and legal challenges related to jurisdiction, data sovereignty, and contracts with providers. Academic literature confirms that cloud forensics has become one of the most active research areas (Alenezi et al., 2024).

Another major trend is the increasing use of artificial intelligence and automation in digital investigation processes. Industry reports indicate a rise in investment in AI-assisted sorting, automated artifact analysis, and SaaS investigation platforms (Magnet Forensics, 2025; Cellebrite, 2025). The rationale is clear: investigators are faced with exponentially growing volumes of data, and manual analysis is no longer viable at scale. However, it is important to critically assess this trend. AI-generated results in a digital investigation context raise significant questions of explainability, reproducibility, and admissibility. If a machine learning model flags a file or communication as significant, the analyst must be able to justify this conclusion in a legally credible manner. The opacity of some AI systems can conflict with the evidentiary standards required in legal proceedings, and the field currently lacks clear frameworks and professional consensus on this issue (Kävrestad, 2024). A third trend is the growing importance of mobile and remote forensic analysis, with smartphones remaining among the most evidence-rich devices in many investigations, and corporate environments increasingly requiring data collection via the network rather than the physical seizure of devices.

Key Challenges

Despite these advances, digital forensics still faces major challenges. Robust encryption remains one of the most visible technical obstacles, particularly in mobile environments where end-to-end encrypted messaging applications leave very little data recoverable. Another challenge lies in the volume and diversity of data. Investigators may have to deal with logs, cloud artifacts, browsing histories, application databases, memory dumps, and deleted files, often from multiple devices simultaneously. Cloud investigations introduce further complications, including issues of resource sharing, incomplete access to provider-controlled logs, and complex cross-border legal questions regarding data access and admissibility (Alenezi et al., 2024; Kävrestad, 2024).

There is also a professional challenge worth highlighting. The sector increasingly demands practitioners who combine technical skills, methodological rigor, legal knowledge, and communication abilities. The concrete relevance of these challenges became particularly clear during my personal monitoring of cybersecurity news in January and February 2026. Several documented incidents during this period highlighted recurring patterns directly related to digital forensics practices. In January 2026, the active re-exploitation of a five-year-old vulnerability in the Fortinet SSL VPN (CVE-2020-12812), affecting more than 10,000 unpatched firewalls, demonstrated how outdated systems continue to pose serious risks to investigations. That same month, the Kimwolf botnet, which compromised more than two million connected devices worldwide and transformed them into nodes in a residential proxy network, underscored the growing

complexity of tracing malicious infrastructure across distributed and consumer-grade endpoints. In February 2026, the continued exploitation of a directory traversal vulnerability in WinRAR, disclosed six months earlier, along with a critical Telnet vulnerability actively targeting operational technology environments in the manufacturing, healthcare, and government sectors, confirmed that unpatched enterprise software remains a primary source of forensic analysis requests. These examples underscore that digital forensics is now fully integrated into cybersecurity operations and no longer confined to traditional post-crime incident analysis (Cybersecurity Personal Surveillance, January and February 2026).

National and International Job Market

The job market confirms that digital forensics is a relevant and rapidly growing professional sector. In the UK, the government report "Cybersecurity Skills in the UK Job Market 2025" highlights a persistent and structural skills shortage. This report estimates that approximately 44% of UK businesses lack basic cybersecurity skills and that demand for specialist roles, particularly in digital forensics and incident response, consistently outstrips supply. Job postings in 2026 confirm recruitment for roles such as digital forensics investigator, DFIR analyst, and incident response consultant. Salaries for experienced professionals typically range from £45,000 to £80,000 per year, depending on seniority and sector (Indeed, 2026).

Internationally, the picture is equally positive. In continental Europe, the implementation of NIS2 and DORA regulations is generating increased demand for digital forensics skills within financial institutions and critical infrastructure operators. Multinational consulting firms offer dedicated digital forensics and cyber investigation services, with international recruitment. This sector is also experiencing strong growth in North America. This confirms that digital forensics has largely moved beyond police laboratories and specialized law enforcement units to become integrated into a broader professional ecosystem linked to cyber defense, compliance, and business resilience (UK Government, 2025).

Conclusion

In conclusion, digital forensics has become a broad and strategic discipline at the crossroads of investigation and cybersecurity. It now encompasses cloud, mobile, memory, and enterprise environments, and relies on increasingly sophisticated tools for forensic analysis and incident response. At the same time, this field faces significant technical, legal, and organizational challenges, particularly regarding encryption, cloud complexity, AI transparency, and the reliability of evidence. The integration of digital forensics into routine cybersecurity operations, coupled with a persistent skills shortage and increasing regulatory pressure in the UK and internationally, makes it a highly relevant field with real career prospects for recent cybersecurity graduates (NIST, 2024; UK Government, 2025).

References

- Alenezi, A. et al. (2024) Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. MDPI. Available at: <https://www.mdpi.com/1424-8220/24/2/433>
- Cellebrite (2025) Industry Trends Survey 2025. Available at: <https://cellebrite.com/en/industry-trends-survey-2025/>
- Cellebrite (2025) UFED. Available at: <https://cellebrite.com/en/products/ufed/>
- DFRWS (2024) DFRWS EU 10-year Review and Future Directions in Digital Forensic Research. Available at: https://www.dfrws.org/wp-content/uploads/2024/03/DFRWS-EU-10-year-review-and-future-direct_2024_Forensic-Science-Internationa.pdf
- Indeed (2026) Digital Forensic Jobs in the UK. Available at: <https://uk.indeed.com/q-digital-forensic-jobs.html>
- Kävrestad, J. (2024) Fundamentals of Digital Forensics. Springer. Available at: <https://link.springer.com/book/10.1007/978-3-031-53649-6>
- Magnet Forensics (2025) Magnet AXIOM. Available at: <https://www.magnetforensics.com/products/magnet-axiom/>
- Magnet Forensics (2025) State of Enterprise DFIR Report 2025. Available at: <https://www.magnetforensics.com/resources/state-of-enterprise-dfir-2025-report/>
- NIST (2024) SP 800-201: Cloud Computing Forensic Reference Architecture. Available at: <https://csrc.nist.gov/pubs/sp/800/201/final>
- UK Government (2025) Cyber Security Skills in the UK Labour Market 2025. Available at: <https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2025>
- Velociraptor (2025) Overview. Available at: <https://docs.velociraptor.app/docs/overview/>

Personal research material

Personal cyber news monitoring notes (January–February 2026), compiled from public cybersecurity reporting. Used as contextual background to illustrate recurring incident patterns in relation to forensic practice.