

Digital Forensics: Current State, Tools, Cybersecurity Integration, Emerging Trends, Challenges and Job Market

*Task 1 Research Report | Module: ACCA7031 Digital
Forensics Analysis*

Submitted by

MD Imran Biswas

Student ID: 2436882

University of Wales Trinity Saint David

Table Of Content

1. Introduction.....	2
2. Current State of Digital Forensics.....	2
3. Tools, Features and Capabilities	3
4. Intersection with Digital Forensics and Cybersecurity	4
5. Emerging Trends in Digital Forensics	4
6. Key Challenges	4
7. National and International Job Market	5
8. Conclusion	5
References	6

1. Introduction

In the last 20 years, digital forensics has changed dramatically from being a small group of law-enforcement experts to being a key component of the cybersecurity industry. The science of digital forensics is fundamentally concerned with Digital Evidence identification, preservation, analysis and presentation in a legally admissible and reproducible way [1]. The amount and type of digital evidence has grown in tandem with the sophistication of computing devices that are used in all but the most mundane activities in our daily lives, from smartphones to cloud services to industrial control systems and sensors from the Internet of Things (IoT). This report views the field, its key tools, its relationship to cybersecurity, emerging trends, important challenges and the career landscape both domestically and internationally.

2. Current State of Digital Forensics

The field of digital forensics has come a long way, with internationally accepted standards, certifications, and body of peer-reviewed research. There are also a number of frameworks to support investigators in their approach to evidence handling, including the ACPO Good Practice Guide for Digital Evidence (UK) and the guidelines from the National Institute of Standards and Technology (NIST) [2]. However, as noted by Zareen et al. [1] the pace of technological advancement is still rapid and is outstripping forensic practice, as has been noted many times previously.

There are many sub-disciplines in the field today, including disk forensics, memory forensics, network forensics, mobile device forensics and, more recently, cloud and IoT forensics. There are unique acquisition issues for each sub-domain and specialized tool sets for each. Moreover, the current landscape of digital forensics has evolved beyond the reactive after-executed phase of an incident or malicious activity and has become a more comprehensive and proactive part of the security operations, with the new area of Digital Forensics and Incident Response (DFIR) [3] being an example.

3. Tools, Features and Capabilities

There is a wide range of forensic tools available to support forensic investigators from different evidence types and operational situations. Table 1 below provides a summary of 7 popular tools, the main purpose they serve and the most important features.

Table 1: Commonly Used Digital Forensic Tools and Their Capabilities

Tool	Type	Key Capabilities	Deployment
Autopsy / Sleuth Kit	Disk & File Forensics	Forensic imaging, deleted file recovery, hash verification, timeline analysis, keyword search	Open-source; Windows/Linux
FTK Imager	Acquisition Tool	Bit-for-bit forensic imaging, MD5/SHA-1 hashing, live RAM capture, write-blocking support	Commercial (free tier); Windows
Cellebrite UFED	Mobile Forensics	Physical/logical extraction from iOS/Android, app data recovery, GPS artefacts, cloud extraction	Commercial; field deployment
Magnet AXIOM	Integrated Platform	Artefact correlation, cloud evidence acquisition, mobile & computer analysis, AI-assisted triage	Commercial; enterprise
Volatility	Memory Forensics	RAM dump analysis, process injection detection, rootkit identification, network connection artefacts	Open-source; cross-platform
Wireshark	Network Forensics	Packet capture & analysis, protocol dissection, traffic reconstruction, anomaly detection	Open-source; cross-platform
EnCase	Enterprise Forensics	Large-scale evidence processing, eDiscovery, legal reporting, remote acquisition, GDPR compliance	Commercial; enterprise

The Sleuth Kit is the basis for Autopsy, an open-source tool that is routinely used in the legal profession and in academic research. Commercial tools, however, like Magnet AXIOM and EnCase provide enterprise-level evidence management, automated artefact correlation and built-in legal reporting – features that can be especially important when investigating complex corporate incidents or handling a large eDiscovery project. Cellebrite UFED is still the top mobile device extraction solution and has been used by police around the world [3]. Memory forensics stands out as an area of volatility where investigators can uncover rootkits and process injection methods that are hard to find with disk-based forensics. These tools can be used in a complementary manner; normally if evidence exists it will be from multiple tools, not a single tool.

4. Intersection with Digital Forensics and Cybersecurity

Cyber Forensics and Forensics are becoming more and more intertwined. The DFIR model is a single operation construct that integrates threat hunting, containment and forensics evidence preservation [3]. As a result, forensic specialists often work closely with Security Operations Centre (SOC) personnel while an incident is still in progress and when carrying out incident post-mortems.

Digital forensics supports security by: 1) reconstructing time lines and visualizing attack entry, movement and exit vectors; 2) examining malware through memory forensics and sand-boxing techniques; and 3) evidence collection that is conducive to accountability and admissibility (in civil and criminal legal proceedings). But Du et al. [5] warn that the need to respond quickly is competing with evidence preservation, and that the DFIR process exists to balance the need for response speed with the preservation of evidence.

5. Emerging Trends in Digital Forensics

Digital forensics is evolving in several ways. The adoption of cloud computing, often multi-tenant environments by business organizations means that cloud forensics has gained in importance but challenges with cross-jurisdiction issues, shared storage systems and data retention policies make obtaining evidence difficult [6]. IoT forensics continues to grow, while at the same time issues around the heterogeneity of devices, restricted memory and proprietary firmware make it hard to support IoT forensics with existing tools [7].

Another development is the use of artificial intelligence (AI) for forensics triage. Machine learning methods can be used to automate log filtering, anomaly detection and image categorization that can speed up the analysis of large sets of evidence [5]. While the lack of explanatory power of AI is a concern, this could also lead to problems in the legal environment since the forensic rationale behind any conclusion needs to be clear and transparent [8]. Another trend is forensics in blockchain and cryptocurrency, particularly in regard to financial crimes. The standardization of procedures in the exchange of evidence across borders at international level is also being studied [6] and so is forensic automation.

6. Key Challenges

Digital Forensics is regarded as one of the segments of the cybersecurity market. The report UK Cyber Security Skills in the UK Labour Market 2025, commissioned by the UK Government reported that only 8% of the cyber businesses surveyed had digital forensics as a specific area of expertise, which is the least prevalent specialism [9]. The same report also revealed the average salary for a base cyber security job in London 2024 was £55,000, and then topped with a London weighting of £11,000. Careers range from work in law enforcement agencies, regulatory agencies, incident response and containment companies, security operations Centre and eDiscovery companies [9][10].

The forensics skills demand is there in North America, Europe and Asia-Pacific markets. The following are the most common job descriptions in this area: Digital Forensic Analyst, Cyber Incident Responder, Malware Analyst, SOC Analyst, and eDiscovery Specialist [10]. Employers look for a candidate with experience using forensic tools and understanding the artefacts from both Windows and Linux environments, as well as experience with mobile and cloud forensics, some Python or PowerShell experience and knowledge of evidential admissibility in court, and good report writing skills [9][10].

7. National and International Job Market

Digital forensics is a growing area within cybersecurity. The UK Government's Cyber Security Skills in the UK Labour Market 2025 report states that only 8% of surveyed UK cyber businesses had digital forensics as a workforce specialism, making it the least used specialism [9]. The same report shows that core cybersecurity roles in London had a median salary of £55,000 in 2024, plus an £11,000 London premium. Career paths include law enforcement, regulatory agencies, incident response firms, cybersecurity teams, and eDiscovery roles [9][10].

International demand is also strong in North America, Europe, and Asia-Pacific. Common roles include Digital Forensic Analyst, Cyber Incident Responder, Malware Analyst, SOC Analyst, and eDiscovery Specialist [10]. Employers usually seek forensic tool experience, Windows/Linux artefact knowledge, mobile and cloud forensics, Python or PowerShell skills, legal evidence handling, and report writing [9][10].

8. Conclusion

Digital forensics is a rapidly evolving field that is technically complex and plays a growing role in cybersecurity and related legal actions. The tools being used in the field have become more advanced, with the integration of platforms and the use of artificial intelligence in analysis that helps solve some of the issues involved in scalability for investigators. But encryption, anti-forensics, cloud jurisdiction and IoT heterogeneity are still huge challenges. Incorporation of cybersecurity into DFIR, and the continued demand for practitioners who possess both forensic technical skills and a legal perspective and can respond to incidents has broadened the scope of the profession. As cyber threats become more complex, the need for strong and well-qualified Digital Forensics practitioners should not cease to increase.

References

- [1] M. S. Zareen, B. Aslam, S. Tahir, I. Rasheed, and F. Khan, "Unveiling the Dynamic Landscape of Digital Forensics: The Endless Pursuit," *Computers*, vol. 13, no. 12, p. 333, Dec. 2024, doi: <https://doi.org/10.3390/computers13120333>.
- [2] National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response*, NIST SP 800-86. Gaithersburg, MD: NIST, 2006. [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-86/final>
- [3] SANS Institute, "Digital Forensics and Incident Response," SANS.org, 2024. [Online]. Available: <https://www.sans.org/cybersecurity-focus-areas/digital-forensics-incident-response>
- [4] I. Ismail and K. Akram, "The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance," *PLoS ONE*, vol. 20, no. 9, pp. e0331683–e0331683, Sep. 2025, doi: <https://doi.org/10.1371/journal.pone.0331683>.
- [5] X. Du et al., "SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation," in *Proc. 15th Int. Conf. Availability, Reliability and Security (ARES)*, 2020. [Online]. Available: <https://arxiv.org/abs/2012.01987>
- [6] Alshabibi, Munirah Maher, Bu, and H. Rahman, "Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review," *Computers*, vol. 13, no. 8, p. 213, Aug. 2024, doi: <https://doi.org/10.3390/computers13080213>.
- [7] Abdulghani Ali Ahmed, K. Farhan, W. A. Jabbar, Abdulaleem Al-Othmani, and Abdullahi Gara Abdulrahman, "IoT Forensics: Current Perspectives and Future Directions," *Sensors*, vol. 24, no. 16, pp. 5210–5210, Aug. 2024, doi: <https://doi.org/10.3390/s24165210>.
- [8] R. Montasari et al., "A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response," *Forensic Sciences Research*, 2023. [Online]. Available: <https://arxiv.org/pdf/2309.07064>
- [9] Department for Science, Innovation and Technology, "Cyber Security Skills in the UK Labour Market 2025," GOV.UK, 2025. [Online]. Available: <https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2025>
- [10] Forensic Focus, "Digital Forensics Jobs Round-Up, October 13 2025," *ForensicFocus.com*, Oct. 2025. [Online]. Available: <https://www.forensicfocus.com/jobs/digital-forensics-jobs-round-up-october-13-2025/>