

Digital Forensics: A Research Report

Current State, Trends, Challenges, and Career Opportunities

Orneda Kamberi | 2526289 | ACCA7031 - Digital Forensics Analysis

University of Wales Trinity Saint David | April 2026

1. Introduction

Digital forensics is the process of collecting, preserving, and analysing digital evidence to support legal investigations ^[1]. It has grown quickly in recent years because of the increase in cybercrime and the use of digital devices in everyday life. This report provides an overview of the current state of digital forensics, including the tools available, how it connects to cybersecurity, emerging trends, the main challenges faced by investigators, and the job opportunities available in the field.

2. Current State of the Field: Tools and Capabilities

Digital forensic investigators today have access to a wide range of professional tools. Cellebrite UFED is one of the most widely used tools for mobile phone forensics. It allows investigators to perform physical and logical extractions from Android and iOS devices, recovering deleted data, communication logs, GPS metadata, and application data ^[2]. Autopsy is a popular open-source platform used to analyse forensic images. It supports keyword searching, file carving, metadata extraction, and communication analysis, and is compatible with images acquired using other tools ^[3].

FTK (Forensic Toolkit) by Exterro is another industry standard used for disk imaging and analysis. FTK Imager specifically is used to create verified forensic images in E01 format with MD5 and SHA-1 hash verification, which is important to prove that evidence has not been changed ^[4]. Hashcat is a widely used password recovery tool, which can crack encrypted files using methods such as brute-force, dictionary, and hybrid attacks. These tools together form the core of a modern forensic investigation toolkit.

According to Carrier ^[5], one of the most important capabilities in modern forensics is the ability to recover deleted files through file carving, a technique that searches for known file headers in unallocated disk space. This is particularly useful when suspects have tried to delete evidence before their devices are seized.

3. Intersection of Digital Forensics and Cybersecurity

Digital forensics and cybersecurity are closely linked. While cybersecurity focuses on preventing attacks, digital forensics focuses on investigating what happened after a breach

has occurred ^[6]. In practice, many organisations need both skills working together. When a security incident takes place, forensic investigators are called in to identify how the attacker gained access, what data was accessed, and what tools were used.

This relationship is sometimes called Cyber Forensics or Incident Response Forensics. Casey ^[7] explains that forensic analysis during an incident response can help organisations understand the full scope of an attack and take steps to prevent it from happening again. Tools like SIEM (Security Information and Event Management) systems and endpoint detection platforms now often include forensic capabilities, which shows how the two fields are becoming more integrated.

The Computer Misuse Act 1990 ^[8] and the General Data Protection Regulation (GDPR) ^[9] also create a legal link between forensics and cybersecurity, as organisations are required to investigate breaches and report them to authorities. This means that forensic evidence must be collected properly to be admissible in court.

4. Emerging Trends in Digital Forensics

Several important trends are shaping the future of digital forensics. One of the most significant is cloud forensics. As more organisations move their data to cloud platforms such as AWS, Microsoft Azure, and Google Cloud, investigators increasingly need to recover evidence from remote servers rather than physical devices ^[10]. This creates new challenges because data may be stored across multiple jurisdictions.

Artificial intelligence (AI) is also beginning to be used in digital forensics. AI tools can help analysts sort through large volumes of data more quickly, identify patterns, and flag suspicious files automatically ^[11]. This is particularly useful in cases involving millions of files. However, the use of AI in forensics also raises questions about transparency and reliability of automated findings in court.

Another growing area is IoT (Internet of Things) forensics. Devices such as smart home speakers, wearables, and connected cameras can contain valuable evidence. Zawoad and Hasan ^[12] note that these devices present unique challenges because they often have limited storage and non-standard operating systems that are harder to analyse with traditional tools.

5. Key Challenges

Despite advances in tools and techniques, digital forensics faces a number of serious challenges. Encryption is one of the biggest. Modern devices and communication platforms increasingly use end-to-end encryption, which can make it very difficult or impossible to

access data even when a device has been seized legally ^[13]. Tools like Hashcat can help in some cases, but strong encryption may remain unbreakable.

The volume of data that investigators must process is also growing rapidly. A single smartphone can contain hundreds of thousands of files. Sorting through all of this data to find relevant evidence requires significant time and computing resources ^[4]. Anti-forensic techniques, such as file wiping, steganography, and the use of privacy-focused operating systems like Tails or Kali Linux, are also being used more frequently by suspects to hide their activities ^[14].

Legal and jurisdictional issues present another challenge. When evidence is stored in another country, investigators may need to go through lengthy legal processes to access it. This can delay investigations significantly. Additionally, the chain of custody must be carefully maintained at all times, as any break in this chain can make evidence inadmissible in court ^[1].

6. National and International Job Market

The demand for digital forensics professionals is growing both in the UK and internationally. In the UK, roles in digital forensics are available in law enforcement agencies such as the National Crime Agency (NCA) and police forces, as well as in private sector companies and consultancies. The NCA regularly recruits for roles including Digital Forensic Investigator and Cybercrime Analyst ^[15].

Internationally, the job market is particularly strong in the United States, where organisations such as the FBI, CISA, and large technology companies actively hire forensic analysts. According to the US Bureau of Labor Statistics, employment in information security, which includes digital forensics, is expected to grow by 33% between 2023 and 2033, much faster than the average for other occupations ^[16].

Job portals such as LinkedIn, Indeed, and CyberSecurityJobs.com regularly advertise roles with titles such as Digital Forensic Analyst, Incident Response Analyst, and Malware Analyst. Employers commonly require knowledge of tools such as Autopsy, FTK, and Cellebrite, along with relevant certifications such as GCFE (GIAC Certified Forensic Examiner), EnCE (EnCase Certified Examiner), or CFCE (Certified Forensic Computer Examiner) ^[17].

7. Conclusion

Digital forensics is a field that is growing and changing quickly. New tools, particularly those using AI and cloud-based investigation, are making investigators more effective.

However, the challenges are growing at the same pace, encryption and anti-forensic techniques mean that investigators cannot rely on tools alone. The close relationship between digital forensics and cybersecurity means that professionals in this field increasingly need skills in both areas. The job market reflects this demand, with strong growth expected in the coming years both in the UK and internationally. As digital evidence plays a greater role in criminal investigations and organisational security, the need for well-trained forensic professionals will continue to rise. To conclude, I would say that digital forensics is no longer a niche specialism, it has become a core part of how organisations and law enforcement respond to the threats of the digital age, and anyone entering this field today is stepping into one of the most relevant and fast-moving areas in technology.

References

- [1] B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations*, 6th ed. Boston: Cengage Learning, 2019.
- [2] Cellebrite, "UFED," Cellebrite, 2024. [Online]. Available: <https://cellebrite.com/en/ufed/> [Accessed Apr. 20, 2026].
- [3] Sleuth Kit Labs, "Autopsy Digital Forensics Platform," 2024. [Online]. Available: <https://www.autopsy.com/> [Accessed Apr. 20, 2026].
- [4] Exterro, "FTK (Forensic Toolkit)," Exterro, 2024. [Online]. Available: <https://www.exterro.com/digital-forensics-software/forensic-toolkit> [Accessed Apr. 20, 2026].
- [5] B. Carrier, *File System Forensic Analysis*. Upper Saddle River: Addison-Wesley, 2005.
- [6] S. Axelsson, "The Base-Rate Fallacy and the Difficulty of Intrusion Detection," *ACM Transactions on Information and System Security*, vol. 3, no. 3, pp. 186–205, Aug. 2000.
- [7] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed. London: Academic Press, 2011.
- [8] *Computer Misuse Act 1990*, ch. 18, London: TSO, 1990. [Online]. Available: <http://www.legislation.gov.uk/ukpga/1990/18/contents> [Accessed Apr. 20, 2026].
- [9] European Parliament, "General Data Protection Regulation (GDPR)," *Official Journal of the European Union*, L 119, May 4, 2016. [Online]. Available: <https://gdpr-info.eu/> [Accessed Apr. 20, 2026].
- [10] S. Zawoad and R. Hasan, "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems," arXiv, 2013. [Online]. Available: <https://arxiv.org/abs/1302.6312> [Accessed Apr. 20, 2026].
- [11] M. Scanlon, "Battling the Digital Forensic Backlog through Data Deduplication," in *Proc. 6th IEEE International Conference on Innovative Computing Technology (INTECH)*, Dublin, Ireland, Aug. 2016.
- [12] S. Zawoad and R. Hasan, "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things," in *Proc. IEEE International Conference on Services Computing (SCC)*, New York, 2015, pp. 279-284.
- [13] J. Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*, 2nd ed. Waltham: Syngress, 2014.

- [14] M. K. Rogers, "Anti-Forensics," in *Handbook of Information and Communication Security*, P. Stavroulakis and M. Stamp, Eds. Berlin: Springer, 2010, pp. 673-682.
- [15] National Crime Agency, "Careers - Digital Forensics Roles," NCA, 2024. [Online]. Available: <https://www.nationalcrimeagency.gov.uk/careers> [Accessed Apr. 20, 2026].
- [16] U.S. Bureau of Labor Statistics, "Information Security Analysts," *Occupational Outlook Handbook*, 2024. [Online]. Available: <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm> [Accessed Apr. 20, 2026].
- [17] GIAC, "GCFE - GIAC Certified Forensic Examiner," GIAC Certifications, 2024. [Online]. Available: <https://www.giac.org/certifications/certified-forensic-examiner-gcfe> [Accessed Apr. 20, 2026].