
RESEARCH REPORT AND DIGITAL FORENSICS PROGRESS REPORT
MOBILE DEVICE FORENSIC INVESTIGATION USING FTK IMAGER AND CELLEBRITE
PHYSICAL ANALYZER

2505249 – SANJAY KUMAR UNKILI
UNIVERSITY OF WALES TRINITY SAINT DAVID – WALES INSTITUTE OF SCIENCE AND ARTS –
School of Applied Computing

ask 1 – Research Report:

Introduction

Digital forensics has evolved into a critical discipline within contemporary cybersecurity and criminal investigations. The increasing sophistication of cyber threats, coupled with the widespread use of mobile devices and digital communication platforms, has transformed the nature of forensic investigations. Modern investigators are expected not only to recover and analyse digital evidence but also to interpret complex patterns of user activity, network interactions, and application behaviour. This report critically examines the current state of digital forensics through the practical use of FTK, Cellebrite UFED, Cellebrite Physical Analyzer, and Autopsy. It further explores the intersection of digital forensics and cybersecurity, emerging technological trends, key challenges, and the national and international job market for forensic professionals.

Current State of Digital Forensics and Forensic Tool Capabilities

The contemporary digital forensic landscape extends far beyond traditional hard-drive examinations. Investigations now routinely involve mobile devices, encrypted storage, cloud-synchronised data, and application-based communications. Consequently, forensic methodologies must combine rigorous evidence preservation with advanced analytical techniques.

FTK remains one of the leading platforms for computer forensic investigations. Its capabilities include forensic imaging, hash verification, keyword searching, deleted file recovery, and the analysis of file system artefacts. FTK is particularly valuable in investigations involving document activity, internet usage, and user-generated content because it enables efficient processing of large datasets while maintaining evidential integrity.

Cellebrite UFED has become a central tool for mobile device acquisition. Modern smartphones contain extensive personal and organisational data, including messages, call records, photographs, application data, and geolocation information. UFED supports both logical and physical extractions, allowing investigators to acquire data from a wide range of mobile operating systems.

Cellebrite Physical Analyzer complements UFED by providing advanced interpretation of extracted data. The platform supports timeline reconstruction, geospatial analysis, communication mapping, and application-level decoding. These features are particularly important in investigations where understanding the sequence of events is as critical as recovering the underlying data.

Autopsy provides a comprehensive open-source environment for forensic analysis. It supports disk image examination, timeline generation, deleted file recovery, and the identification of user activity artefacts. Its modular architecture makes it well suited for both educational and professional investigative environments.

Collectively, these tools demonstrate the current maturity of digital forensics. They enable investigators to conduct integrated examinations across computers and mobile devices while adhering to forensic principles such as chain of custody, reproducibility, and evidence integrity.

Intersection of Digital Forensics and Cybersecurity

Digital forensics and cybersecurity are increasingly interdependent disciplines. Cybersecurity focuses primarily on prevention, detection, and protection, whereas digital forensics provides the investigative capability required to understand how a security incident occurred and what impact it produced.

In a modern incident response environment, forensic analysts work alongside cybersecurity teams to identify attack vectors, establish timelines, determine the scope of compromise, and preserve evidence for legal or regulatory purposes. For example, following a ransomware attack, FTK and Autopsy may be used to examine compromised systems, while UFED and Physical Analyzer can investigate associated mobile communications or authentication activity.

The integration of forensic analysis into cybersecurity operations has also become essential for threat intelligence and post-incident learning. Evidence obtained during forensic investigations can reveal attacker tactics, techniques, and procedures, enabling organisations to improve defensive controls and reduce the likelihood of future compromise. As a result, digital forensics is no longer viewed solely as a post-event investigative function; it is now a strategic component of organisational cyber resilience.

Emerging Trends in Digital Forensics

Several technological developments are reshaping the practice of digital forensics.

Artificial Intelligence and Automated Analysis

Forensic vendors are increasingly incorporating artificial intelligence and machine learning into investigative workflows. These technologies can assist with artefact classification, anomaly detection, and prioritisation of relevant evidence. Automated analysis is particularly valuable when investigators must process large volumes of data under significant time constraints.

Advanced Mobile Forensics

The rapid evolution of mobile applications, encrypted messaging platforms, and cloud-synchronised services has expanded the importance of mobile forensics. Tools such as UFED and Physical Analyzer continue to develop new extraction and decoding capabilities to address emerging mobile operating systems and application architectures.

Cloud-Integrated Investigations

Although local device analysis remains fundamental, many digital artefacts now exist across both physical devices and cloud services. Investigators increasingly need to correlate data recovered from a device with synchronised cloud activity, creating a more holistic understanding of user behaviour.

Timeline-Centric Investigations

Modern forensic investigations place significant emphasis on timeline reconstruction. Rather than analysing artefacts in isolation, investigators seek to establish a coherent sequence of events that explains user actions, data transfers, application usage, and system modifications. Physical Analyzer and Autopsy provide strong support for this investigative approach.

Key Challenges in Digital Forensics

Despite advances in forensic technology, several challenges continue to affect investigative effectiveness.

Challenge	Impact on Investigation
Strong Encryption	Modern devices employ sophisticated encryption mechanisms that can significantly limit data access.

Challenge	Impact on Investigation
Data Volume	Investigators frequently encounter terabytes of information across multiple devices and storage locations.
Anti-Forensic Techniques	Malicious actors may delete logs, use secure wiping tools, or manipulate timestamps.
Rapid Technological Change	New operating systems, applications, and device architectures require continuous adaptation of forensic tools.
Maintaining Evidential Integrity	Investigators must ensure that all acquisition and analysis activities remain forensically sound and reproducible.

These challenges highlight the importance of both technical expertise and methodological discipline. The effectiveness of tools such as FTK, UFED, Physical Analyzer, and Autopsy ultimately depends on the investigator's ability to apply appropriate forensic procedures and interpret the resulting evidence accurately.

National and International Job Market

The demand for digital forensic professionals continues to grow both nationally and internationally due to increasing cybercrime, regulatory requirements, and the expansion of incident response capabilities.

Common roles include:

- Digital Forensic Analyst
- Mobile Forensic Examiner
- Cybercrime Investigator
- Incident Response Analyst
- eDiscovery Specialist

Employers frequently seek candidates with practical experience using industry-standard tools such as FTK and Cellebrite UFED. In the United Kingdom, opportunities exist within law enforcement agencies, government departments, financial institutions, and cybersecurity consultancies. Internationally, countries such as the United States, Canada, Australia, and members of the European Union continue to invest heavily in digital investigation capabilities as cyber threats become increasingly sophisticated.

Conclusion

Digital forensics has developed into a sophisticated investigative discipline capable of analysing computers, mobile devices, and complex digital ecosystems. The practical use of FTK, Cellebrite UFED, Cellebrite Physical Analyzer, and Autopsy demonstrates how contemporary forensic investigations combine evidence acquisition, artefact recovery, timeline reconstruction, and analytical interpretation. The close integration between digital forensics and cybersecurity has transformed forensic analysis into a strategic component of incident response and organisational resilience. Emerging trends such as artificial intelligence, advanced mobile forensics, cloud-integrated investigations, and timeline-centric analysis continue to expand investigative capabilities.

Nevertheless, significant challenges remain, including encryption, data volume, anti-forensic techniques, and the rapid pace of technological change. Addressing these challenges requires not only advanced forensic tools but also a rigorous understanding of forensic methodology, evidential integrity, and investigative reasoning.

References

- [1] AccessData, *Forensic Toolkit (FTK) User Guide*. AccessData, 2024. [Online]. Available: <https://accessdata.com/>
- [2] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 4th ed. Cambridge, MA, USA: Academic Press, 2024.
- [3] Cellebrite, *UFED and Physical Analyzer Documentation*. Cellebrite, 2024. [Online]. Available: <https://cellebrite.com/>
- [4] B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations*, 7th ed. Boston, MA, USA: Cengage Learning, 2023.
- [5] National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response (SP 800-86)*. Gaithersburg, MD, USA: NIST. [Online]. Available: <https://csrc.nist.gov/>
- [6] The Sleuth Kit, *Autopsy Digital Forensics Platform Documentation*. [Online]. Available: <https://www.autopsy.com/>