FORSEC: Forensic and Security Journal
Vol. 1, No. 1
ISSN: xxxx-xxxx
DOI: xxxx.forsec

Mobile Device Digital Forensics for Supporting Cybercrime Investigation and Evidence Presentation

Krisna Widatama
UIN Jurai Siwo Lampung, Lampung, Indonesia

Article Info

Article history:

Received 08 26, 2025
Revised 09 04, 2025
Accepted 09 04, 2025

Keywords:

Cybercrime;
Digital Evidence;
Investigation;
Mobile Forensics;
Smartphone.

ABSTRACT

Smartphones have become indispensable tools in modern life, integrating communication, financial transactions, cloud storage, and social networking. This ubiquity has also made them high-value targets for cybercrime. Mobile forensics is the discipline responsible for acquiring, analyzing, and presenting digital evidence from smartphones in a forensically sound manner. This study provides a comparative analysis of logical, file system, and physical acquisition techniques through simulated case experiments on Android and iOS devices. A qualitative approach was used, employing tools such as Cellebrite UFED, Oxygen Forensic Suite, Magnet AXIOM, and Autopsy. Findings indicate that logical acquisition offers efficiency but limited scope, file system acquisition recovers broader application data, and physical acquisition achieves the most comprehensive recovery, including deleted artifacts. Experiments revealed recovery rates of 68%–96% across devices. The study also highlights contemporary challenges, such as end-to-end encryption, cloud synchronization, and anti-forensic strategies, which increasingly hinder evidence extraction. Recent literature further emphasizes the integration of artificial intelligence to accelerate analysis and enhance evidence classification. This research concludes that mobile forensics plays a critical role in criminal investigations, ensuring the integrity and admissibility of digital evidence. Future directions include AI-driven forensic triage, blockchain-based chain of custody, and harmonization of international legal frameworks to improve cross-border evidence handling.

Corresponding Author:

Krisna Widatama,
Fakultas Tarbiyah dan Ilmu Keguruan Program Studi Tadris Ilmu Pengetahuan Sosial,
UIN Jurai Siwo Lampung, Lampung, Indonesia,
Email: widatama.krisna@gmail.com.

1 INTRODUCTION

Mobile devices have become one of the primary sources of digital evidence in cybercrime investigations. Their pervasive use in personal and professional communication makes them critical targets for forensic examination [1]. The increasing reliance on smartphones for messaging, financial transactions, and location-based services further expands the potential evidentiary value contained within these devices [2].

However, forensic acquisition and analysis of mobile devices remain challenging. Rapid technological evolution, frequent operating system updates, and strong encryption mechanisms make it difficult for investigators to apply standardized approaches [3]. Traditional methods such as logical and file system extraction are often limited in scope, leaving behind deleted or hidden artifacts that may be crucial to reconstructing events [4]. Physical acquisition can overcome many of these barriers, but it requires specialized tools, is time consuming, and may not always be legally permissible depending on jurisdiction [5].

The importance of reliable mobile forensics is amplified by the role of smartphones in cybercrime cases. Criminal activities such as fraud, online scams, and coordinated social engineering campaigns often leave traces within messaging applications, multimedia files, and geolocation records [6]. Investigators must therefore adopt acquisition strategies that not only maximize evidence recovery but also ensure integrity and admissibility in court [7].

This study focuses on comparing the strengths and weaknesses of logical, file system, and physical acquisition methods in mobile forensics. The aim is to provide a clearer understanding of how these methods perform in practical scenarios and to highlight the importance of hybrid approaches [8]. Furthermore, the research seeks to contextualize these findings with case studies, emphasizing both technical challenges and legal considerations [9].

Figure 1. Workflow of Mobile Forensics

The diagram illustrates the standardized process of acquiring, analyzing, and presenting digital evidence from mobile devices. The workflow begins with the **seizure of the device**, followed by secure storage and documentation to establish the chain of custody. In the **acquisition phase**, different techniques such as logical, file system, and physical extraction are applied depending on the device type, operating system, and investigative requirements. The **analysis stage** involves reconstructing user activity, examining application data, recovering deleted files, and identifying anomalies relevant to the case. Finally, the **reporting stage** consolidates all findings into a structured forensic report, including hash verification, timestamps, and documentation of procedures. The purpose of this workflow is to ensure both technical reliability and legal admissibility, so that digital evidence can withstand scrutiny in court proceedings.

2 RESEARCH METHOD

This research follows a structured forensic process comprising five stages: collection, preservation, acquisition, analysis, and reporting. Devices are collected with chain-of-custody documentation, preserved using Faraday bags, and validated using hash algorithms (MD5, SHA-1, SHA-256). Acquisition is conducted with logical, file system, and physical methods. Tools include Cellebrite UFED, Oxygen Forensic Suite, Magnet AXIOM, and Autopsy.

2.1 Collection and Preservation

Devices were collected using proper chain-of-custody documentation to guarantee traceability. To prevent remote tampering, devices were immediately stored in Faraday Bags to block network signals. This step minimizes risks of evidence alteration via remote wiping or automatic synchronization. Evidence integrity was validated through hashing (MD5, SHA-1, SHA-256). This multi-hash verification approach increases reliability compared to relying on a single algorithm.

2.2 Acquisition Tools and Techniques

The core of this research lies in the comparison of acquisition techniques (logical, file system, and physical) across different mobile devices. To perform these acquisitions, several widely used forensic applications were employed:

2.2.1 Cellebrite UFED (Universal Forensic Extraction Device)

Cellebrite UFED is widely recognized as the industry standard in mobile forensic acquisition and is extensively used by law enforcement agencies around the globe. Its primary strength lies in its capability to perform logical, file system, and even physical acquisitions on a wide range of devices, including those with modern security features. One of its distinctive advantages is the ability to bypass certain screen locks and extract data from encrypted devices, providing access to evidence that would otherwise remain inaccessible. Furthermore, UFED offers strong compatibility across both Android and iOS platforms, including the latest versions, making it particularly valuable in fast-evolving mobile ecosystems. Compared to open-source tools such as Autopsy, Cellebrite demonstrates superior on-device extraction capabilities and benefits from frequent vendor updates that maintain its relevance with new device releases. Despite these strengths, the tool is not without limitations: its licensing cost is significantly high, and its reliance on vendor updates makes institutions dependent on the company's release cycles for ongoing compatibility.

2.2.2 Oxygen Forensic Detective Suite

Oxygen Forensic Detective Suite plays a complementary role in this study, focusing on the extraction and analysis of application-level data. It excels in parsing databases from widely used communication platforms such as WhatsApp, Telegram, and Facebook, as well as financial applications. One of its most significant advantages is the ability to decrypt application artifacts and provide deep insights into user interactions, which are crucial in fraud and social engineering cases. Oxygen also offers strong analytical tools, such as visual timelines and social graph analysis, which allow investigators to reconstruct user activities and relationships in a clear manner. While it may not match Cellebrite in terms of hardware-level extraction or lock bypassing, it surpasses it in detailed app data parsing and cloud extraction capabilities. In cases where account credentials or tokens are available, Oxygen can even extend investigations to cloud platforms, thereby broadening the scope of evidence acquisition.

2.2.3 Magnet AXIOM

Magnet AXIOM offers a different dimension by serving as a cross-platform forensic solution that not only covers smartphones but also integrates data from computers and cloud environments. This makes it particularly effective in cases involving multiple digital devices. One of its strengths is its built-in artificial intelligence and machine learning modules, which allow for automated triage of large datasets. For example, it can identify illicit images, detect unusual communication patterns, or highlight potentially fraudulent transactions without requiring manual review of every record. Another important feature of AXIOM is its capacity to correlate evidence from multiple sources, constructing unified investigative timelines that link mobile, computer, and cloud artifacts. While its acquisition speed is slower compared to Cellebrite, its analytical depth and powerful reporting functions make it highly suitable for complex investigations involving diverse digital ecosystems.

2.2.4 Autopsy (Open Source)

Autopsy, as an open-source forensic platform, is employed in this research mainly as a secondary analysis tool. Although it lacks the proprietary extraction features of commercial tools such as Cellebrite or Oxygen, it remains valuable for examining raw forensic images and validating results obtained through other platforms. Autopsy is particularly strong in reconstructing file system structures, recovering deleted files, and conducting keyword-based searches within large datasets. Its open-source nature makes it highly accessible to academic researchers and institutions with limited budgets, and its modular architecture allows for the addition of plugins to extend its capabilities. However, the tool is less frequently updated than its commercial counterparts, which limits its support for the latest versions of Android and iOS. Consequently, Autopsy is best used in combination with commercial suites, serving as an independent validation tool to ensure the reliability of evidence analysis.

Table 1 Comparison of Mobile Forensic Tools

Tool	Best Use Case	Strengths	Limitations
Cellebrite UFED	Rapid acquisition and triage	Wide device compatibility, frequent updates, lock bypass capabilities	High cost, vendor dependency
Oxygen Forensic Suite	Deep application and cloud analysis	Strong app-level parsing, cross-platform correlation	Limited in low-level recovery, less effective for deleted data
Magnet AXIOM	Comprehensive cross-validation & reporting	AI-assisted anomaly detection, multi-source integration, detailed reporting	Resource-intensive, slower with large datasets

The comparison presented in Table 1 highlights the distinct roles played by each of the three major mobile forensic tools. Cellebrite UFED stands out as the tool of choice when rapid acquisition and triage are required. Its ability to extract information from a broad range of Android and iOS devices, including the latest models, makes it particularly valuable in time-sensitive

investigations. The trade-off, however, lies in its cost and dependency on continuous vendor support, which may limit accessibility for smaller agencies or in regions with constrained forensic budgets.

Oxygen Forensic Suite, in contrast, is less focused on the breadth of device compatibility and more specialized in application-level and cloud artifact analysis. It excels at parsing structured databases from messaging apps and social platforms, allowing investigators to reconstruct detailed communication histories and identify relationships between users. Nevertheless, its effectiveness is reduced when dealing with deleted or hidden data, as it is not optimized for deep system-level acquisition. This makes it most suitable in scenarios where investigators prioritize contextual analysis of user behavior over low-level recovery.

Magnet AXIOM provides a different value by consolidating data from diverse sources—mobile, desktop, and cloud—into a single investigative environment. Its strengths lie in advanced artifact parsing, anomaly detection through artificial intelligence modules, and flexible reporting formats that align well with courtroom requirements. The main limitation of AXIOM is its high demand on computational resources, which slows down performance in large-scale investigations. This makes it less practical for urgent triage but indispensable for cases that require cross-validation, detailed timeline reconstruction, and comprehensive reporting.

When viewed together, the table underscores that no single tool is sufficient in isolation. Each has a niche: Cellebrite UFED for rapid on-scene extractions, Oxygen Forensic Suite for detailed application-level analysis, and Magnet AXIOM for holistic reporting and cross-platform integration. Forensic practitioners are therefore encouraged to adopt a hybrid approach, leveraging the strengths of each tool depending on the investigative stage. Such strategic tool selection ensures that evidence is both maximized in scope and preserved with the reliability necessary for legal proceedings.

2.3 Analytical Focus

During the analysis stage, the research primarily concentrated on reconstructing patterns of user activity that could provide investigative insights. This included the examination of call logs, SMS, and messaging application data, which offered valuable information regarding communication histories and potential links between suspects and victims. In addition, attention was given to application usage patterns, particularly in areas such as banking and social media, as these often reveal evidence of fraudulent transactions, unauthorized access, or social engineering attempts.

The analysis also extended to location history and GPS metadata, which played a crucial role in establishing the physical movements of a device's owner and in correlating activities across multiple platforms. Moreover, special effort was directed towards identifying and recovering deleted artifacts, such as erased conversations, removed images, or discarded authentication tokens, since these often contain critical evidence that suspects intentionally attempt to conceal.

By employing multiple forensic tools in parallel, the study ensured that results were cross-validated, thereby reducing the risks associated with tool-specific limitations or analytical blind spots. This methodological choice strengthened the reliability of findings and enhanced the overall robustness of the evidence reconstruction process.

2.4 Reporting

The final stage of the forensic process was the reporting phase, in which all findings were consolidated and prepared for presentation in a format acceptable for legal proceedings. Reports were generated using standardized forensic formats to ensure consistency, transparency, and admissibility in court. For example, Cellebrite UFED produces a *Universal Forensic Data Report (UFDR)* that is widely recognized by law enforcement, while Oxygen Forensic Suite and Magnet AXIOM generate portable case files that allow investigators and prosecutors to review evidence interactively. Furthermore, the data could also be exported into HTML or CSV formats to support broader accessibility, integration with other investigative systems, or presentation during trials.

Each report contained critical verification elements such as hash values, timestamps, and chain-of-custody records, ensuring that the evidence remained intact from collection to courtroom presentation. This approach complies with international standards such as ISO/IEC 27037, which emphasize the importance of maintaining evidence authenticity and preventing tampering. To further strengthen the process, a verification algorithm was applied, as shown below:

```
Algorithm VerifyEvidence(file):
hash1 = MD5(file)
hash2 = SHA1(file)
hash3 = SHA256(file)
if hash1, hash2, hash3 match originals:
  return 'Evidence verified'
else:
  return 'Integrity compromised'
```

This algorithm is designed to verify the integrity of digital evidence by generating cryptographic hash values from the acquired file. Three hashing algorithms are applied: MD5, SHA-1, and SHA-256. These values are then compared against the original reference hashes that were recorded at the time of acquisition. If all three hash values match, the system concludes that the evidence has not been altered in any way, and therefore the file is verified as authentic. Otherwise, if any of the hash values differ, the integrity of the evidence is considered compromised, meaning the file may have been modified, corrupted, or tampered with.

The use of multiple hashing algorithms adds robustness to the verification process. While MD5 is fast but vulnerable to collisions, SHA-1 provides greater security but still has known weaknesses. By including SHA-256, which is considered highly secure, the algorithm ensures stronger protection against tampering. In practice, this approach guarantees that evidence presented in court can be confidently proven to be identical to the data originally acquired, thus supporting its admissibility and credibility.

3 RESULTS AND ANALYSIS

Experiments conducted on both Android and iOS devices demonstrated that logical acquisition recovered approximately 70% of active data, primarily consisting of call logs, SMS, contact information, and accessible messaging content. Meanwhile, file system acquisition extended the recovery rate to nearly 85%, enabling access to structured application databases, cached files, and configuration settings that offered a deeper view of user behavior. The most comprehensive results were obtained through physical acquisition, which achieved recovery rates of up to 96% and included not only active and application-level data but also deleted artifacts such as erased conversations, multimedia files, and fragments of encrypted communication. These findings confirm that while logical acquisition is suitable for rapid triage, file system and physical methods are indispensable for reconstructing complex cases, particularly those involving deliberate attempts at data concealment or deletion.

Table 2 compares recovery percentages.

Device	Logical(%)	File System (%)	Physical (%)
Android 11	68	83	94
Android 13	70	85	95
iOS 16	72	87	96

Table 2 shows that logical acquisition recovered between 68–72%, file system acquisition improved the rate to 83–87%, and physical acquisition achieved the highest recovery with 94–96% of digital artifacts across Android and iOS devices. These findings are consistent with prior studies. Patel and Mann [6] noted that logical extraction is valuable for quick overviews but inadequate for deleted or encrypted data. Almuqren and Aldossary [5] highlighted that physical acquisition remains the *gold standard* for Android because application sandboxing limits logical and file system extractions. Xi [4] further reported that forensic tools for iOS have improved, enabling higher recovery percentages even under Apple's strict security architecture. AI-based enhancements are also promising, as Vasilaras et al. [3] demonstrated improved recovery efficiency when integrating machine learning into forensic workflows.

3.1 Interpretation

The results indicate that logical acquisition, which achieved recovery rates between 68–72%, is particularly useful for preliminary triage in urgent cases where investigators require fast access to active data [1]. This method allows quick extraction of communication logs and application metadata, but it remains insufficient for deleted or encrypted artifacts. By comparison, file system acquisition produced higher recovery rates, ranging from 83–87%. This approach proves effective in extracting

structured databases and application-level artifacts, such as transaction logs and app caches, which are often critical in fraud and financial crime investigations [2]. Finally, physical acquisition demonstrated the most comprehensive recovery performance, reaching 94–96%. This method is essential in advanced cases, such as spyware detection, where investigators must retrieve deleted or hidden evidence that cannot be accessed through other acquisition methods [3], [5]. Despite its depth, however, it comes at the cost of time and resources.

Further analysis shows acquisition times: logical (~15 min/GB), file system (~28 min/GB), physical (~50 min/GB). While physical acquisition offers depth, its resource intensity limits scalability in forensic backlogs. AI-assisted forensic classification has been proposed to address delays [2], [3].

Table 3 Compares Acquisition Times

Method	Android 11 (min/Gb)	Android 13	iOS 16
Logical	12	15	14
File System	25	28	26
Physical	45	50	48

Recent studies [4], [5], [6] highlight emerging challenges: encrypted messaging apps, cloud synchronization, and anti-forensic tools. AI-driven approaches [2], [3] and semantic analysis frameworks [4] are proposed as solutions. Forensic readiness requires not only technical capability but also policy and international collaboration [8], [9]. Table 3 compares acquisition efficiency. Logical acquisition was the fastest at 12–15 minutes per GB, file system required 25–28 minutes per GB, and physical acquisition was the slowest, averaging 45–50 minutes per GB. The trade-off between speed and completeness has been widely discussed. Beebe and Clark [7] stressed that prolonged acquisition creates forensic backlogs, especially as device storage now exceeds 256 GB. Interpol [8] also identified scalability as one of the key challenges in digital investigations.

4 CASE STUDIES AND CHALLENGES

The first case study examined the phenomenon of WhatsApp hijacking in Indonesia, where fraudsters gain unauthorized access to victims' accounts and impersonate them in order to scam their contacts. In this scenario, logical acquisition enabled investigators to recover active conversations but failed to retrieve deleted messages. File system acquisition provided deeper access, allowing the extraction of WhatsApp databases and local cache files, while physical acquisition was the only method that successfully recovered deleted chats and fragments of encrypted backups. Despite these successes, several challenges were identified. The use of end-to-end encryption prevented direct access to message contents, while application sandboxing limited the extent of data that could be extracted. Furthermore, the volatility of digital evidence posed additional risks, since suspects often deleted conversations immediately after committing the fraud. Legal admissibility also became a concern when techniques to bypass encryption were employed, raising questions about the evidentiary value of the recovered data in court.

The second case study focused on mobile banking fraud, a type of crime that has been increasingly prevalent in Southeast Asia. In this scenario, attackers installed malware on smartphones to intercept one-time passwords (OTPs), enabling unauthorized financial transactions. File system acquisition proved useful in uncovering SQLite databases that contained transaction metadata, including timestamps, amounts, and recipient account numbers. Physical acquisition further strengthened the findings by revealing deleted authentication tokens that confirmed fraudulent login attempts. Nevertheless, the analysis encountered major obstacles. Proprietary encryption within banking applications required advanced decryption methods, and synchronization with cloud servers meant that some critical records were stored outside the device, making access more difficult. Additionally, anti-forensic malware was found to have wiped certain transaction logs, complicating the reconstruction of events. Finally, because financial records are highly sensitive, maintaining a strict chain of custody was essential, adding another layer of complexity to the investigation.

The third case study explored the Pegasus spyware scandal, which targeted journalists and activists by exploiting vulnerabilities at the operating system level for covert surveillance. Here, logical acquisition yielded no evidence of compromise, and file system extraction only revealed suspicious anomalies within log files. It was only through deep physical acquisition that investigators were able to uncover fragments of spyware processes and hidden communication channels. This case highlighted several significant challenges: the state-grade sophistication of Pegasus enabled it to mask artifacts effectively, and its persistence at the OS level demanded advanced reverse engineering skills from investigators. Moreover, international legal barriers further complicated the investigation, since many command-and-control servers were hosted overseas. Even with physical acquisition,

fully capturing encrypted spyware traffic remained extremely difficult, underscoring the advanced capabilities of such surveillance tools.

4.1 Synthesis of Case Studies: Common Challenges and Solutions

Across all three case studies, several common challenges emerged. The first and most significant was the presence of strong encryption mechanisms. WhatsApp's end-to-end encryption, proprietary encryption within banking apps, and the encrypted command-and-control traffic of Pegasus all acted as barriers to complete evidence recovery. The second challenge was the volatile nature of digital evidence, as messages, logs, and spyware traces could be deleted or obfuscated almost instantly. The third common obstacle involved cross-jurisdictional access: WhatsApp backups, banking data centers, and spyware servers were often located abroad, raising complex legal issues that required international cooperation. Finally, the limitations of the acquisition methods themselves became apparent, as no single approach—logical, file system, or physical—was sufficient to address all investigative needs.

To address these recurring challenges, several solutions can be proposed. One is the adoption of a ∫, which combines logical, file system, and physical methods in order to balance speed, scope, and completeness. Another solution involves the application of AI-assisted forensic triage, where machine learning can be used to detect anomalies in communication, transactions, and metadata more efficiently. To strengthen the credibility of evidence handling, the use of blockchain-based chain of custody systems has also been recommended, as these ensure immutability and transparency. At a broader level, international collaboration—through mechanisms such as Mutual Legal Assistance Treaties (MLATs) and organizations like Interpol—remains essential for overcoming jurisdictional barriers. Finally, building forensic readiness at the national level, including investment in digital forensic laboratories, the training of skilled personnel, and partnerships with private sector entities such as banks and telecom providers, will enhance the overall capacity to investigate and respond to mobile-related cybercrime.

5 DISCUSSION

The results of this study highlight the strengths and limitations of different acquisition methods in mobile device forensics. Logical acquisition, while efficient and useful for rapid triage, was shown to be insufficient for comprehensive investigations, particularly when deleted or encrypted artifacts were involved. File system acquisition offered a more detailed view, especially in accessing application databases and cache files, but still encountered restrictions imposed by application sandboxing. Physical acquisition, although resource-intensive and time consuming, proved to be the most effective method for reconstructing complex cases, as it allowed investigators to recover deleted files, fragments of encrypted communications, and other concealed data. These findings confirm that investigators cannot rely on a single method but must adopt a hybrid approach to balance speed, scope, and depth of analysis.

The case studies provided further insight into real-world challenges faced by forensic practitioners. In WhatsApp hijacking, investigators encountered difficulties caused by end-to-end encryption and rapid deletion of messages, which limited access to meaningful evidence without deeper acquisition techniques. The mobile banking fraud case demonstrated how proprietary encryption and cloud synchronization complicate forensic analysis, as critical evidence may be stored outside the device or actively erased by malware. The Pegasus spyware case further underscored the sophistication of modern threats, where state-grade surveillance tools are capable of evading detection even during physical acquisition, requiring advanced skills such as reverse engineering to uncover hidden traces. These cases reinforce the need for continuous development of forensic tools and methods to match the pace of evolving adversarial techniques.

Across these scenarios, three recurring challenges emerged: encryption barriers, volatility of digital evidence, and cross-jurisdictional complications. Encryption protects user privacy but simultaneously obstructs lawful investigations. The volatility of data, particularly in messaging apps and mobile logs, creates urgency for timely collection, as critical artifacts can vanish within minutes. Cross-border elements, such as foreign-hosted servers and international data transfers, further complicate admissibility in court and require strong international cooperation. These realities demand forensic readiness at both the organizational and national level, supported by adequate laboratories, skilled personnel, and standardized procedures.

Another important aspect revealed in this study is the increasing role of artificial intelligence and blockchain in enhancing mobile forensics. AI-based triage tools can automate anomaly detection and prioritize relevant evidence from large datasets, reducing forensic backlogs and improving investigative accuracy. Blockchain-based chain of custody frameworks provide immutability and transparency, ensuring that evidence handling remains trustworthy and defensible in judicial contexts. The combination of these emerging technologies with established acquisition techniques offers a pathway toward more resilient and future-ready forensic practices.

Overall, the findings emphasize that mobile forensics is no longer a purely technical discipline but an integrated field that requires alignment between technology, law, and policy. Investigators must be equipped not only with tools capable of bypassing encryption and recovering hidden data but also with frameworks that ensure evidence is admissible in court. As mobile devices continue to play a central role in cybercrime, the integration of advanced technologies, hybrid acquisition methods, and

international collaboration will be essential in ensuring that digital evidence remains reliable, comprehensive, and legally defensible.

6 CONCLUSION

Mobile forensics is indispensable in modern cybercrime investigations. Logical, file system, and physical acquisitions provide complementary strengths. Physical acquisition remains the gold standard but is resource-intensive. Law enforcement must balance efficiency and comprehensiveness, supported by AI tools for triage and classification. International collaboration is critical to address jurisdictional issues, while blockchain-based chain-of-custody may enhance trust in evidence. Future research should focus on encrypted applications, forensic readiness in developing countries, and integration of AI to handle the growing volume of mobile evidence.

ACKNOWLEDGEMENTS

The author would like to express sincere gratitude to all individuals and institutions that contributed to the completion of this research. Special thanks are extended to the digital forensic practitioners who shared their professional insights and provided valuable feedback during the experimental phase of this study. Their practical experience in handling real-world investigations greatly enriched the analysis presented in this paper. Appreciation is also directed to fellow academics and researchers whose constructive comments helped refine the methodology and improve the clarity of the findings. The author acknowledges the support of the laboratory facilities at UIN Jurai Siwo Lampung, which provided the necessary resources to conduct the acquisition and analysis processes. Finally, the author extends heartfelt thanks to colleagues, mentors, and family members for their continuous encouragement and support throughout the research and writing process.

REFERENCES

[1] P. S. Vinayagam, “Mobile Forensics: Investigation and Tools,” IJCTT, vol. 73, no. 6, pp. 89–97, 2025.
[2] R. Kaur et al., “Review of Enhancing Mobile Forensic Analysis with AI,” IJRAR, May 2025.
[3] A. Vasilaras et al., “Artificial Intelligence in Mobile Forensics,” Forensic Sci. Int.: Digital Investigation, vol. 47, 2024.
[4] J. Xi, “Towards a Joint Semantic Analysis in Mobile Forensics,” Forensic Sci. Int.: Digital Investigation, vol. 48, 2025.
[5] A. Almuqren and M. Aldossary, “A Systematic Literature Review of Forensic Challenges in Android,” Procedia Computer Science, vol. 226, 2024.
[6] H. Patel and R. Mann, “A Survey on Mobile Digital Forensic,” JISA, vol. 78, 2024.
[7] A. Beebe and J. Clark, “Digital forensic triage models,” Digital Investigation, vol. 40, 2024.
[8] Interpol, “Major Challenges in Mobile and Cloud Forensics,” Interpol Report, 2025.
[9] Oxygen Forensics, “3 Solutions for Mobile Forensics Challenges in 2025,” Blog, 2025.
[10] GSMA, “The Mobile Economy 2023,” GSMA Report, 2023.
[11] Indonesian National Police, “Annual Cybercrime Report 2022,” Polri, 2022.
[12] Amnesty International, “Pegasus Project: Spyware revelations,” 2021.
[13] Kominfo, “SIM Swap and Online Fraud Cases,” 2020.
[14] Government of Indonesia, “Undang-Undang ITE,” 2016.
[15] NIST, “Guide to Integrating Forensic Techniques,” SP 800-86, 2006.