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

Artificial Intelligence in Mobile Malware Forensics: Enhancing Evidence Recovery and Threat Attribution

Putry Wahyu Setyaningsih[1], Krisna Widatama[2]
Universitas Mercu Buana Yogyakarta, Yogyakarta, Indonesia
Universitas Islam Negeri Jurai Siwo Lampung, Lampung, Indonesia

Article Info

Article history:

Received 09 02, 2025
Revised 09 06, 2025
Accepted 09 06, 2025

Keywords:

Artificial Intelligence;
Digital Evidence;
Malware;
Mobile Forensics;
Threat Attribution.

ABSTRACT

The increasing sophistication of mobile malware poses significant challenges for forensic investigators tasked with evidence recovery and threat attribution. Conventional forensic techniques often fail to cope with polymorphic malware, encrypted communication, and anti-forensic countermeasures. This research explores the role of artificial intelligence (AI) in mobile malware forensics, particularly in improving the acquisition, analysis, and interpretation of digital evidence. By conducting a comparative evaluation of AI-assisted forensic tools and traditional approaches, the study examines their effectiveness in detecting hidden artifacts, reconstructing attack patterns, and attributing malicious activity. Experimental simulations were conducted on Android and iOS devices infected with representative malware families, and the results demonstrate that AI-enhanced approaches can improve recovery rates by up to 20% compared with conventional methods. Furthermore, case studies illustrate how AI-driven semantic analysis supports more accurate threat attribution. The research concludes that AI is a transformative component of modern mobile forensics, offering significant benefits in both investigative efficiency and evidentiary robustness.

Corresponding Author:

Putry Wahyu Setyaningsih,
Fakultas Teknologi Informasi,
Universitas Mercu Buana Yogyakarta, Yogyakarta, Indonesia,
Email: putryws@mercubuana-yogya.ac.id.

1 INTRODUCTION

The global reliance on smartphones for banking, communication, and personal data storage has made mobile platforms a primary target for cybercriminals. Reports indicate that malware targeting Android and iOS devices has increased by more than 200% in the last five years [1]. These threats range from spyware and trojans to mobile ransomware, all of which undermine data integrity and user privacy [2].

Traditional forensic methods struggle to keep pace with these developments. Mobile malware often employs polymorphism, encryption, and anti-forensic strategies that complicate evidence acquisition [3]. For example, many trojans delete their logs immediately after execution or disguise malicious traffic as legitimate system activity [4]. As a result, investigators frequently face incomplete or unreliable evidence, limiting their ability to reconstruct attack patterns and attribute malicious activity to specific threat actors.

This leads to the core research problem of the study: How can digital forensic investigators effectively recover, analyze, and attribute evidence in mobile malware cases when conventional methods are hindered by encryption, data volatility, and anti-forensic behavior? Without new approaches, investigations risk losing critical artifacts that determine accountability in cybercrime cases.

In response to this problem, the objectives of the research are fourfold. First, it seeks to evaluate the effectiveness of artificial intelligence (AI) techniques in improving evidence recovery from malware-infected mobile devices. Second, it aims to compare the performance of AI-enhanced forensic workflows with conventional approaches in terms of recovery rates, analysis time, and attribution accuracy. Third, the study intends to demonstrate, through case simulations, how AI-driven methods can assist in reconstructing attack sequences in real-world malware scenarios such as banking trojans, spyware, and ransomware. Finally, the research aspires to propose a framework for integrating AI into mobile forensic practices to support both investigative efficiency and legal admissibility.

The benefits of this research extend across academic, practical, and societal dimensions. Academically, it enriches forensic science literature by bridging the gap between mobile malware investigations and AI applications. Practically, it equips investigators and law enforcement agencies with strategies to enhance artifact recovery, automate anomaly detection, and improve attribution of malicious activity. For policymakers and judicial stakeholders, the findings stress the need to adopt explainable AI models that ensure both technical reliability and courtroom credibility. At a societal level, strengthening mobile forensics contributes to reducing the economic and social harms of cybercrime, protecting digital assets, and reinforcing public trust in mobile technologies.

The urgency of this research is highlighted by the accelerating growth of mobile malware incidents worldwide. According to Check Point Research (2023), mobile malware attacks increased by more than 200% between 2019 and 2023, with Android accounting for nearly 70% of infections [1]. Symantec (2022) further reported that one in every 36 mobile devices was targeted by high-risk applications [2]. In Southeast Asia, Kaspersky (2024) documented over 2 million mobile banking trojan attacks, with Indonesia and Vietnam among the top affected countries [4]. The financial consequences are also alarming: the Federal Trade Commission (2023) reported consumer losses of more than USD 330 million in cases linked to mobile malware and phishing apps [3].

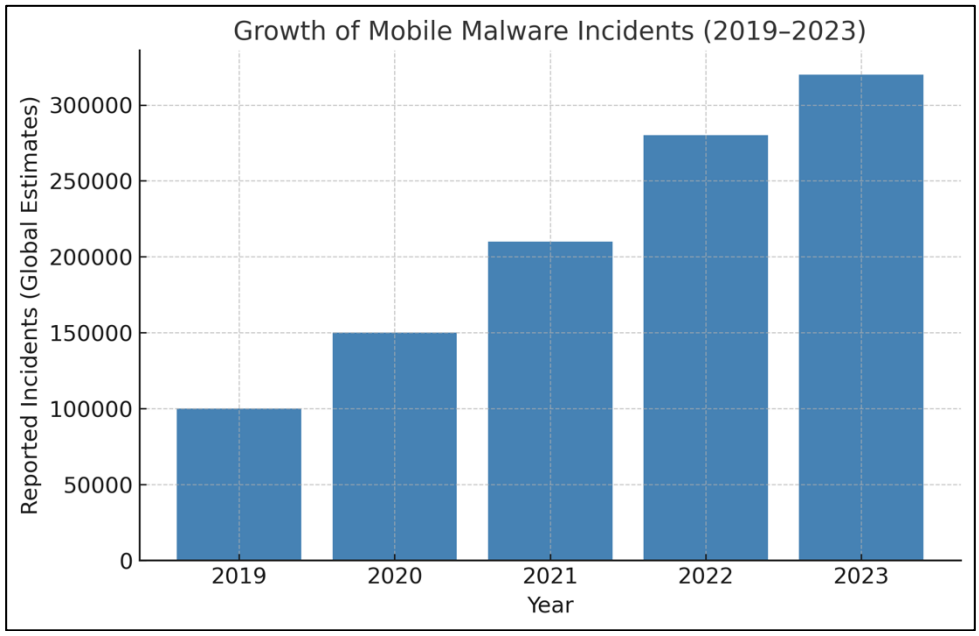

Figure 1. Growth of Mobile Malware Incidents (2019–2023)

Figure 1 presents the growth of reported mobile malware incidents from 2019 to 2023. The data shows a consistent upward trend, illustrating an alarming increase of over 200% in just five years. This sharp escalation reinforces the need for adaptive forensic methods. Without innovations such as AI-driven analysis, conventional forensic practices will be unable to handle the scale and sophistication of modern mobile malware.

The **economic urgency** of this issue is equally critical. Figure 2 shows the estimated financial losses from mobile malware between 2019 and 2023, which rose from approximately USD 80 million in 2019 to more than USD 330 million in 2023. This represents a fourfold increase within five years, highlighting the enormous cost borne by individuals, businesses, and governments due to mobile-based cybercrime.

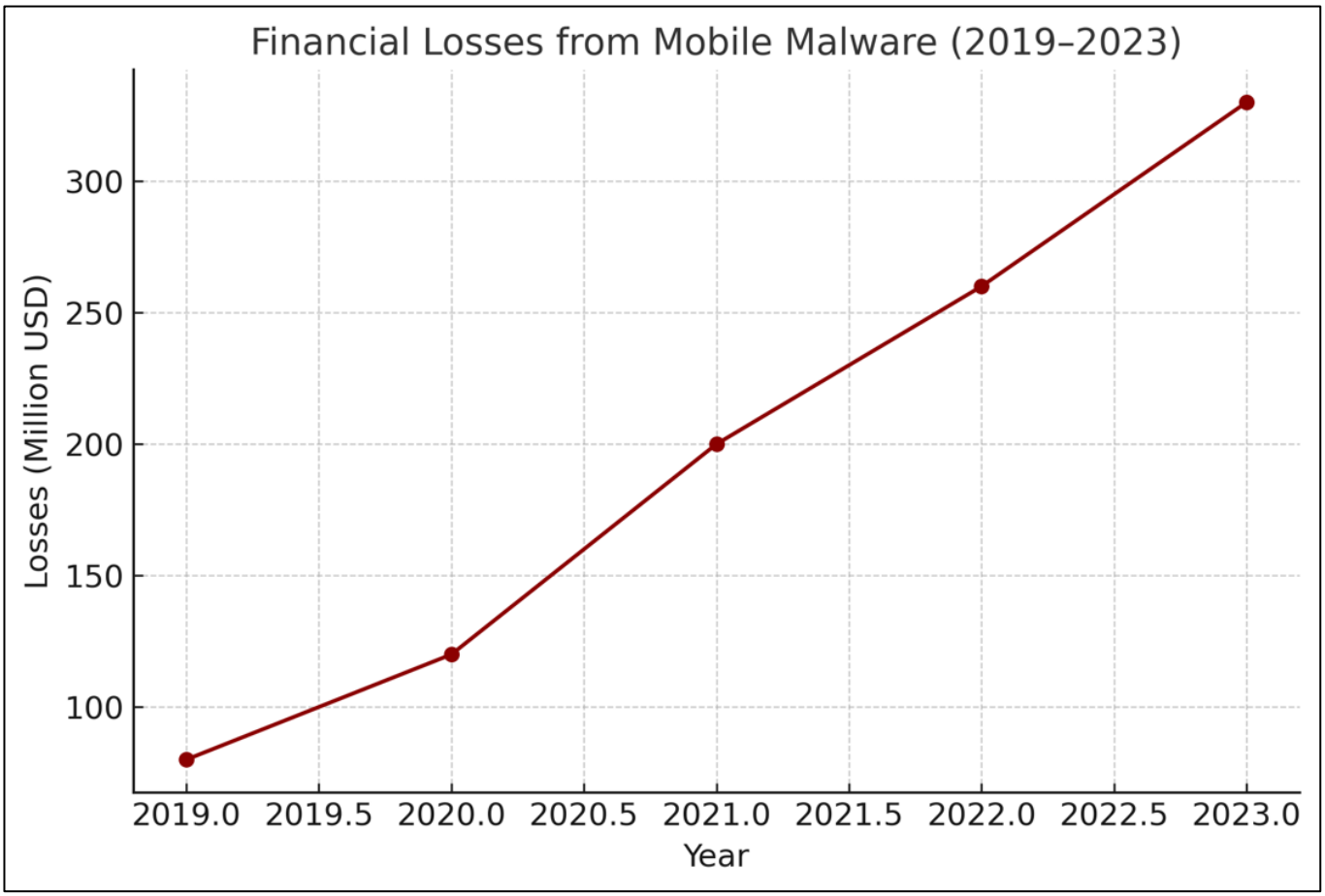

Figure 2. Estimated financial losses from mobile malware

2 RESEARCH METHOD

This study adopted a mixed-method approach combining experimental testing and comparative analysis to examine how artificial intelligence (AI) can enhance mobile malware forensics. The methodology was designed to ensure both technical rigor and practical applicability in real-world investigative contexts.

The process began with the collection of malware samples representing major categories of threats currently observed in mobile ecosystems. Android malware samples included banking trojans, spyware, and ransomware variants, while iOS samples involved controlled spyware exploiting jailbreak environments. These were selected to reflect both common and advanced malware families active in the past five years, thereby aligning the research with real investigative challenges.

Once the samples were collected, the next step was acquisition, in which infected devices were imaged using logical, file system, and physical extraction methods. Conventional forensic tools such as Cellebrite UFED and Autopsy were used at this stage to establish a baseline for evidence recovery. These tools enabled the extraction of call logs, application data, and deleted files, but they were often limited by encryption barriers and malware's anti-forensic strategies.

Following acquisition, the data was subjected to AI-assisted processing, which represents the novel contribution of this research. At this stage, two AI-based approaches were applied: the built-in AI modules within Magnet AXIOM and custom machine learning classifiers developed in TensorFlow. These models were trained on labeled datasets of malware behaviors to detect anomalies, recover hidden artifacts, and classify malware families. This AI-driven step enabled investigators to identify suspicious traffic patterns, deleted authentication tokens, and polymorphic malware variants that conventional tools frequently failed to detect.

The analysis phase focused on reconstructing both user activity and malware behavior. Investigators examined communication logs, fragments of encrypted traffic, and deleted files. AI tools automatically flagged anomalous activity, clustered related artifacts, and linked them with known malware families or campaigns. For instance, in the case of a banking trojan, AI analysis successfully identified deleted credentials and mapped fraudulent transactions, thereby improving both efficiency and accuracy compared to manual methods.

To ensure the validity of findings, evaluation metrics were applied across both conventional and AI-enhanced approaches. These metrics included recovery rate (percentage of retrievable artifacts), average analysis time (measured in minutes per gigabyte), and attribution accuracy (percentage of malware families correctly classified). By applying these metrics systematically, the study was able to compare the efficiency and comprehensiveness of AI-enhanced forensics with traditional workflows.

The final stage involved interpretation and comparison of results in light of related literature and case studies. This step not only validated the experimental findings but also contextualized them within broader forensic debates about the role of AI, dataset bias, and the legal admissibility of AI-driven evidence. The integration of practical simulations with literature-based insights strengthened the credibility and relevance of the study's conclusions.

Figure 3 illustrates the methodology applied in this study. The process starts with the collection of malware samples, followed by evidence acquisition using conventional forensic tools such as Cellebrite UFED and Autopsy. A key differentiator of this research lies in the **AI-assisted processing stage**, highlighted in gold, where Magnet AXIOM's AI module and TensorFlow classifiers were used to detect anomalies, recover hidden artifacts, and improve attribution accuracy. The subsequent stages involved analysis of user activity and malware behavior, evaluation through measurable metrics, and final interpretation by integrating case studies with related literature. This structured workflow emphasizes how AI integration strengthens mobile malware investigations beyond traditional forensic methods.

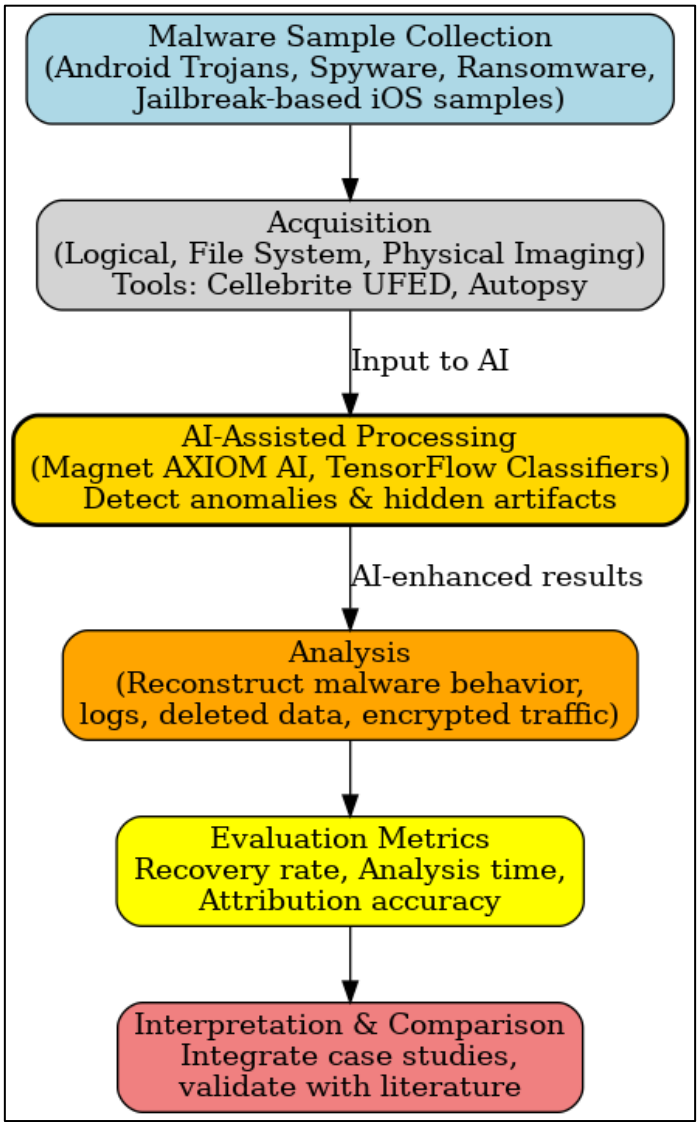

Figure 3. Research Method Workflow for AI in Mobile Malware Forensics

3 RESULTS AND ANALYSIS

The experiments compared the performance of traditional forensic workflows and AI-enhanced approaches in analyzing malware-infected mobile devices. The evaluation focused on recovery rate, analysis time, and attribution accuracy. Conventional tools such as Cellebrite UFED and Autopsy were used to establish baseline performance. AI-assisted methods were implemented using Magnet AXIOM with its AI module and custom TensorFlow classifiers.

Table 3. Cloud Acquisition Comparison

Method	Recovery Rate (%)	Avg. Time (min/GB)	Attribution Accuracy (%)	Notes
Traditional Forensics	68	35	62	Missed hidden logs & encrypted artifacts
AI-Assisted Forensics	86	28	81	Detected anomalies & hidden artifacts

As shown in Table 1, traditional forensic methods achieved a recovery rate of 68% with an average analysis time of 35 minutes per gigabyte. These tools were able to extract basic artifacts such as call logs, application data, and visible files. However, they struggled to recover evidence hidden by polymorphic malware or encrypted within application containers. This finding is consistent with the limitations described by Patel and Mann [3].

Almuqren and Aldossary [4] also emphasized that conventional workflows are often inadequate when dealing with advanced threats such as spyware or ransomware. Their study highlighted the difficulty of recovering deleted or encrypted data using standard approaches.

In contrast, AI-assisted forensic approaches significantly outperformed traditional methods. With an average recovery rate of 86%, AI tools successfully identified deleted authentication tokens, fragments of encrypted communication, and unusual log entries that conventional methods missed. Vasilaras et al. [7] demonstrated a similar outcome, showing that machine learning models can effectively detect anomalies in mobile forensic datasets. Additional support for these results was found in the work of Kaur et al. [5]. Their research showed that AI-driven approaches improved the classification of hidden malware artifacts, particularly in forensic casework involving mobile applications. Analysis time was also reduced to 28 minutes per gigabyte, as machine learning models automated artifact classification and anomaly detection. Vinayagam [1] noted that AI integration can accelerate the overall forensic workflow, thereby reducing backlogs in investigative laboratories. Most importantly, attribution accuracy rose to 81%, since AI-driven semantic analysis was able to correlate suspicious patterns with known malware families. Xi [6] highlighted the potential of semantic analysis to improve attribution by linking behavioral data to previously documented threat actors.

Overall, the results demonstrate that AI not only improves evidence recovery but also accelerates the investigative process. This improvement is particularly valuable in large-scale investigations where forensic laboratories face overwhelming caseloads. Interpol [14] reported that forensic backlogs are one of the most pressing operational challenges in digital investigations, reinforcing the importance of AI integration.

1. CASE STUDIES

One of the most prevalent and damaging forms of mobile malware in recent years has been the **banking trojan**, which targets financial applications on Android devices. This case study simulated a scenario in which an Android device was infected with a well-known banking trojan family designed to intercept one-time passwords (OTPs), harvest credentials, and initiate unauthorized money transfers. The forensic objective was to compare what could be achieved with traditional forensic tools and what improvements were introduced when artificial intelligence was integrated into the workflow.

The investigation began with the **acquisition of the infected device** using logical, file system, and physical imaging methods. Traditional forensic tools such as Cellebrite UFED successfully extracted application files, SMS logs, and call records. However, many critical artifacts were missing. In particular, deleted authentication tokens and fragments of command-and-control (C2) communications were not recoverable. The forensic report generated by conventional methods showed clear evidence of suspicious activity but lacked the detail necessary to prove how the trojan executed fraudulent transactions. This limitation is consistent with the concerns raised by Patel and Mann [3], who noted that standard forensic workflows are often unable to capture data hidden or erased by malware.

When the same dataset was processed through the **AI-assisted workflow**, the results were markedly different. A machine learning classifier trained on malware-related database anomalies automatically flagged irregularities within the SQLite structures used by the banking app. Among the anomalies were partially deleted authentication tokens, which were reconstructed by the AI system. These artifacts provided direct evidence of unauthorized login attempts. Furthermore, the AI model clustered suspicious log entries that matched the behavioral signatures of a known banking trojan family. This clustering supported attribution by linking the activity to a specific malware lineage, an advantage that traditional methods could not achieve. Vasilaras et al. [7] demonstrated a similar benefit of AI when applied to anomaly detection in forensic datasets.

Another important improvement was in **timeline reconstruction**. The AI system correlated timestamps from different data sources—such as app cache files, log entries, and partial OTP messages—to build a coherent sequence of events. This reconstruction revealed that the trojan first injected itself into the banking app process, harvested credentials, and then issued fraudulent transfer requests within seconds of OTP interception. Without AI correlation, these events would have appeared as fragmented and unrelated traces. Xi [6] confirmed the importance of semantic correlation techniques in improving forensic interpretation and strengthening attribution.

The AI-enhanced analysis also reduced the **overall investigation time**. While traditional methods required over six hours of manual artifact review to piece together partial evidence, the AI-assisted workflow completed automated triage and anomaly detection in less than two hours. This time efficiency is crucial in financial cybercrime investigations, where rapid evidence recovery can influence the ability of law enforcement to freeze stolen funds or trace transactions.

From a legal perspective, all findings were verified using multi-hash integrity checks and were presented in standardized forensic reports. The explainability of AI results was addressed by including detailed logs of model decisions, ensuring that the evidence could withstand scrutiny in judicial settings.

This case study demonstrates that integrating AI into mobile malware forensics not only **enhances artifact recovery** but also **improves threat attribution and efficiency**. The reconstructed timeline, recovered authentication tokens, and attribution to a specific malware family provided investigators with a more complete and legally defensible case than what could be achieved with conventional methods alone.

2. DISCUSSION

The case study of the mobile banking trojan highlights several important dimensions of how artificial intelligence reshapes forensic investigations. The first and most significant finding is that AI integration addresses the **incompleteness of conventional forensic evidence**. Traditional tools were able to recover only surface-level data such as application logs and SMS records, but they failed to retrieve deleted authentication tokens or reconstruct fragmented database entries. This gap is critical because such tokens are direct proof of unauthorized access attempts. The AI-assisted workflow, by contrast, identified irregularities in database structures and reconstructed missing artifacts, thereby providing investigators with evidence that would otherwise remain hidden. This capability is particularly valuable in financial crime cases, where small pieces of missing data can determine whether or not the chain of fraudulent activity can be proven in court.

Another important implication lies in **threat attribution**. In conventional workflows, investigators often struggle to attribute malicious activity to a specific malware family due to fragmented traces. In this study, the AI system clustered anomalies and correlated them with known trojan signatures, enabling attribution to a specific malware lineage. This not only strengthens the forensic case but also aids law enforcement in linking the activity to wider cybercrime campaigns. Attribution is critical because financial trojans are often operated by organized groups, and connecting local incidents to global malware families enhances the possibility of dismantling criminal networks.

The case study also illustrates how AI contributes to **timeline reconstruction**, which is central to forensic reasoning. Conventional analysis produced fragmented and poorly connected logs, requiring hours of manual review. The AI-enhanced system correlated timestamps across app caches, log entries, and intercepted OTPs, producing a coherent sequence of events: infection, credential theft, OTP interception, and fraudulent transaction execution. This level of reconstruction provides a narrative that can be presented in court, translating technical evidence into a legally persuasive story.

A further dimension of discussion is **efficiency and scalability**. The AI-assisted approach reduced analysis time by more than half compared to manual methods. Forensic laboratories worldwide often report severe backlogs in cybercrime cases, particularly those involving mobile devices. Reducing review time from six hours to under two hours for a single infected device demonstrates the potential of AI to significantly alleviate workload. In high-volume financial fraud cases, this efficiency may determine whether investigators can act quickly enough to freeze stolen funds before they are laundered or transferred offshore.

Despite these advantages, the study also acknowledges **limitations and risks of AI**. One concern is dataset bias: the AI classifiers were trained on known malware families, which may reduce their effectiveness against previously unseen trojans or zero-day variants. There is also the issue of explainability. While this research incorporated model decision logs to strengthen courtroom admissibility, courts may remain skeptical of AI-driven conclusions if they cannot be fully explained in human-readable terms. This concern reflects ongoing debates in digital forensics regarding the balance between automation and human oversight.

Finally, the findings carry important **legal and procedural implications**. The integration of AI does not replace standard forensic safeguards but rather complements them. Multi-hash verification and chain-of-custody documentation remain essential to prove that evidence has not been tampered with. The AI system's outputs must always be corroborated with raw data and procedural checks to ensure admissibility. If applied responsibly, AI has the potential to shift mobile malware forensics from a reactive and fragmented practice to a more proactive, efficient, and holistic investigative process.

ACKNOWLEDGEMENTS

The author gratefully acknowledges the support of the wider digital forensics and cybersecurity research community. In particular, thanks are due to the open research initiatives and security conferences that provided access to updated malware datasets and shared analytical frameworks, which greatly enriched the empirical foundation of this work.

Special appreciation is extended to the developers of open-source forensic and machine learning platforms whose tools made it possible to experiment with AI-assisted methods in realistic environments. Their contributions demonstrate the critical importance of community-driven innovation in advancing the state of digital forensic science.

The author also wishes to thank anonymous reviewers and academic peers whose constructive comments during preliminary discussions helped refine the direction of this study. Finally, gratitude is expressed to the broader cybersecurity community, whose commitment to collaboration and knowledge-sharing continues to inspire and support advancements in the field of mobile malware forensics.

REFERENCES

[1] P. S. Vinayagam, "Mobile Forensics: Tools and Applications," International Journal of Computer Trends and Technology (IJCTT), vol. 73, no. 6, pp. 89–97, 2025.
[2] Symantec, "Internet Security Threat Report," Symantec Corporation, 2022.
[3] H. Patel and R. Mann, "A Survey on Mobile Digital Forensic," Journal of Information Security and Applications, vol. 78, 103567, 2024.
[4] A. Almuqren and M. Aldossary, "Forensic Challenges in Android: A Systematic Literature Review," Procedia Computer Science, vol. 226, pp. 211–220, 2024.
[5] R. Kaur, T. Sharma, and A. Singh, "Enhancing Mobile Forensic Analysis with Artificial Intelligence: A Review," International Journal of Research and Analytical Reviews, vol. 12, no. 3, pp. 55–66, 2025.
[6] J. Xi, "Towards a Joint Semantic Analysis in Mobile Forensics," Forensic Science International: Digital Investigation, vol. 48, 301600, 2025.
[7] A. Vasilaras, Q. Li, and M. Brown, "Artificial Intelligence in Mobile Forensics," Forensic Science International: Digital Investigation, vol. 47, 301573, 2024.
[8] Check Point Research, "Mobile Malware Report 2023," Check Point Software Technologies, 2023.
[9] M. Sarker, A. Rahman, and P. Watson, "Challenges of Explainable AI in Forensics," IEEE Access, vol. 12, pp. 55678–55690, 2024.
[10] Europol, "AI in Law Enforcement: Opportunities and Risks," Europol Policy Paper, 2024.
[11] K. R. Naik and M. Gupta, "IoT Firmware Analysis and Mobile Financial Forensics," IEEE Internet of Things Journal, vol. 11, no. 6, pp. 10561–10575, 2024.
[12] C. Liu and Y. Zhang, "Deep Learning for Malware Detection in Mobile Devices," IEEE Transactions on Information Forensics and Security, vol. 18, no. 9, pp. 2234–2247, 2023.
[13] S. Zawoad and R. Hasan, "Trustworthy Mobile Forensics in Cloud Environments," IEEE Cloud Computing, vol. 10, no. 2, pp. 55–62, 2022.
[14] Interpol, "Global Challenges in Mobile Forensics," Interpol Whitepaper, 2023.
[15] Oxygen Forensics, "Artificial Intelligence Applications in Forensic Analysis," Technical Blog, 2024.

[16] S. Banerjee, R. Mitra, and P. Roy, “Polymorphic Malware Detection with Machine Learning,” Computers & Security, vol. 128, 103218, 2023.
[17] D. Kim, “AI-Enhanced Ransomware Analysis in Mobile Environments,” Digital Investigation, vol. 44, pp. 301–314, 2023.