Attacks on Mobile Devices and Their Forensics: A Survey

Mrs. Shruti S. Gosavi[1], Dr. Anup Girdhar[2]
[1]*Research Scholar, Tilak Maharashtra Vidyapeeth*
[2]*Research Guide, Tilak Maharashtra Vidyapeeth*
doi.org/10.64643/IJIRTV12I7-188057-459

***Abstract*—Mobile devices have evolved from simple communication tools into indispensable platforms for banking, e-commerce, entertainment, and enterprise applications. Their ubiquity and always-connected nature make them attractive targets for attackers. Adversaries exploit vulnerabilities in operating systems, applications, networks, and even user behavior to compromise confidentiality, integrity, and availability of data. The rapid evolution of attack vectors demands equally advanced forensic techniques to preserve, acquire, and analyze digital evidence in a legally admissible manner. This survey provides a comprehensive overview of mobile attack taxonomies, forensic investigation methodologies, and tools. It highlights challenges including encryption, cloud storage, and device heterogeneity. Additionally, the paper reviews recent research contributions and outlines emerging trends such as artificial intelligence, blockchain for evidence integrity, and privacy-preserving forensic frameworks. By synthesizing literature and practices, this survey aims to assist both researchers and practitioners in understanding the dynamic landscape of mobile security and digital forensics.**

***Index Terms*—Mobile Security, Mobile Forensics, Cyber Attacks, Malware, Digital Evidence, Cloud Forensics, Blockchain, Artificial Intelligence**

I. INTRODUCTION

Mobile devices have become the central computing platform for billions of users. Reports indicate that more than 6.5 billion smartphones were in active use by 2023, with continuous growth projected [1]. These devices store personal communications, multimedia, financial credentials, health records, and sensitive enterprise data. Their versatility encompassing GPS, sensors, high-speed processors, and wireless interfaces makes them both powerful and vulnerable.With this expansion, attackers have increasingly targeted mobile platforms. Malicious campaigns range from banking trojans and spyware-as-a-service to nation-state surveillance malware. Unlike traditional desktop environments, mobile devices face constraints such as limited battery, fragmented operating systems, and diverse hardware ecosystems, complicating both attack mitigation and forensic examination.

Mobile forensics has emerged as a crucial discipline within digital forensics. Defined as the process of recovering digital evidence from mobile devices under forensically sound conditions, it involves acquisition, preservation, analysis, and reporting [2]. Law enforcement agencies rely on forensic methodologies not only to investigate cybercrime but also to gather admissible evidence for courts of law.

II. CONTRIBUTIONS OF THIS SURVEY

1. It presents a taxonomy of mobile attacks supported by real-world examples.
2. It synthesizes forensic approaches and tools, emphasizing acquisition challenges.
3. It identifies open challenges and future research directions, bridging gaps between academic research and practical needs.

III. REAL-TIME MOBILE ATTACKS

Year	Mobile Malware Incidents	Phishing Attacks	Ransomware Cases	Infected Devices	Source
2019	1,500,000+	150,000+	5,000+	320M+	Kaspersky Security Report
2020	2,100,000+	235,000+	12,500+	450M+	Trend Micro Mobile Threat Report
2021	3,200,000+	485,000+	28,000+	580M+	AV-TEST Institute Data
2022	5,400,000+	780,000+	45,000+	720M+	Zimperium Global Report
2023	7,800,000+	1,200,000+	62,000+	890M+	Lookout Mobile Threat Report
2024	9,200,000+	1,850,000+	85,000+	1.1B+	Verizon Mobile Security Index
2025 (H1)	5,600,000+	1,100,000+	48,000+	650M+	Kaspersky H1 2025 Report

Table 1: Year-wise Real-Time Statistics of Mobile Attacks (2019-2025)

IV. KEY OBSERVATIONS FROM REAL-TIME DATA

The data presented in Table 1 reveals several critical trends in mobile security threats (Kaspersky, 2025; Verizon, 2025; Zimperium, 2024):

- Exponential Growth. Mobile malware incidents increased by approximately 287% from 2019 to 2024, reflecting the growing attractiveness of mobile platforms as attack targets.
- Phishing Dominance. Phishing attacks demonstrated the steepest growth trajectory, with a 1,133% increase over six years, making it the most prevalent attack vector in 2024-2025.
- Ransomware Acceleration. Ransomware cases targeting mobile devices increased by 1,600% from 2019 to 2024, reflecting organized cybercriminal adaptation to mobile platforms.
- Device Infection Rates. The total infected devices globally grew from 320 million in 2019 to 1.1 billion in 2024, representing a 244% increase in compromised endpoints.
- 2025 Trend. The first half of 2025 shows a continued threat landscape with 9.2 million malware incidents detected year-to-date, with phishing remaining the dominant attack method.

V. LITERATURE REVIEW

Several surveys have addressed mobile security and forensic challenges. Hoog [6] pioneered forensic studies focusing on Android platforms, highlighting techniques for recovering SMS, call logs, and file systems. Casey [7] provided foundational principles of digital evidence handling, which remain relevant in mobile investigations.

Alghafli et al. [8] reviewed forensic tools, noting discrepancies in extraction results across commercial suites like UFED and XRY. Jain and Singh [9] highlighted forensic challenges in the face of encryption and frequent OS updates. More recently, Chen et al. [10] examined kernel-level exploits and their forensic implications, while Daryabar et al. [11] investigated cloud forensic scenarios, emphasizing the importance of correlating evidence between devices and cloud storage.

Despite this progress, gaps remain. Many studies focus on either security mechanisms or forensics, but rarely provide a holistic view combining attack surfaces with forensic countermeasures. Furthermore, emerging areas such as AI-driven analysis, wearable forensics, and privacy-preserving approaches remain underexplored. This survey addresses these gaps by integrating perspectives from both domains.

VI. CATEGORIZATION OF MOBILE ATTACKS

Mobile attacks can be broadly categorized into five classes: malware-based, network-based, application-level, OS/hardware exploits, and social engineering. Each class contains unique subcategories, as detailed below.

VII. MALWARE-BASED ATTACKS

Mobile malware remains the most pervasive threat. Types include:

1. Trojans Disguised as legitimate apps (e.g., BankBot targeting Android banking apps)
2. Spyware Collects user activities, location, and keystrokes (e.g., Pegasus, attributed to state-level actors)
3. Ransomware Locks devices or encrypts files (e.g., LockerPin ransomware on Android)
4. Adware Aggressively displays ads, draining resources
5. Worms Self-propagating malware spreading via Bluetooth or messaging apps

The forensic challenge lies in detecting residual artifacts, as sophisticated malware often employs obfuscation, encryption, and self-deletion mechanisms.

VIII. NETWORK-BASED ATTACKS

Mobile devices continuously interact with cellular networks, Wi-Fi, and Bluetooth. Key threats include:

- Man-in-the-Middle (MITM) Attackers intercept communication over unsecured Wi-Fi
- Rogue Access Points Fake Wi-Fi hotspots lure victims for data interception
- Base Station Imitation Rogue cell towers (IMSI catchers) capture calls and messages
- SIM Cloning/Spoofing Allows impersonation of legitimate users

Forensics must often extend beyond device logs to network packet captures and telecom provider records.

IX. APPLICATION-LEVEL ATTACKS

Applications constitute a primary attack surface. Examples include:

- Malicious Apps Hidden payloads masquerading as games or utilities
- Permission Abuse Apps requesting unnecessary access (e.g., flashlight apps demanding contacts access)
- Data Leakage via APIs Poorly designed apps expose sensitive information to external services
- Supply Chain Attacks Legitimate apps compromised during development or updates

Evidence is often found in application logs, sandbox directories, or cloud-synced backups.

X. OS AND HARDWARE EXPLOITS

Mobile operating systems are frequently targeted through:

- Privilege Escalation Exploiting vulnerabilities to gain root/jailbreak privileges
- Kernel Exploits Attacks on Android/Linux kernels or iOS kernels
- Baseband Exploits Vulnerabilities in communication chipsets
- Side-channel Attacks Exploiting motion sensors to infer keystrokes

These attacks are harder to detect as they operate at low system levels. Forensic analysis often requires advanced acquisition methods such as chip-off and JTAG.

XI. SOCIAL ENGINEERING ATTACKS

Humans remain the weakest link:

- Phishing/Smishing Fraudulent SMS or emails to steal credentials
- Fake Updates Users tricked into installing security patches that are actually malware
- Deepfake-enabled Scams AI-generated voices or videos impersonate trusted individuals

Forensics focuses on correlating message metadata, timestamps, and user actions.

XII. MOBILE FORENSICS PROCESS AND APPROACHES PHASES OF MOBILE FORENSICS

According to NIST SP 800-101[12], the mobile forensic process includes:

1. Identification Locating potential evidence-bearing devices
2. Preservation Isolating devices from networks (e.g., Faraday bags)
3. Acquisition Extracting data using logical, physical, or advanced methods
4. Analysis Examining files, metadata, deleted data, app artifacts
5. Reporting Preparing court-admissible documentation

XIII. ACQUISITION TECHNIQUES

- Logical Acquisition Extracts accessible data (SMS, call logs). Fast but limited.
- Physical Acquisition Creates a bit-by-bit copy, enabling recovery of deleted data.
- File System Acquisition Captures complete file system, including metadata.
- Advanced Techniques Chip-off, JTAG, and ISP methods used for damaged or locked devices.

XIV. FORENSIC TOOLS

Popular forensic tools include:

- Cellebrite UFED Industry standard for extraction and decoding
- MSAB XRY Specialized in logical and physical acquisitions
- Oxygen Forensic Suite Focused on app and cloud data
- Autopsy/Sleuth Kit Open-source solutions enabling extensible analysis

XV. CASE STUDIES IN MOBILE FORENSICS

- Pegasus Spyware Forensics revealed artifacts in messaging and cache directories [13]
- LockerPin Ransomware Investigators recovered device logs indicating privilege escalation
- IMSI Catcher Evidence Forensic correlation of unusual network activity and baseband logs supported legal cases

XVI. CHALLENGES IN MOBILE FORENSICS

1. Encryption Default full-disk and app-specific encryption complicate acquisition
2. Rapid OS Updates Frequent Android/iOS patches outpace forensic tool updates
3. Cloud Integration Evidence often resides on remote, encrypted servers requiring cross-jurisdiction collaboration
4. Device Heterogeneity Thousands of models and OS versions hinder universal approaches
5. Legal and Privacy Concerns Regulations like GDPR restrict evidence collection
6. Anti-forensic Techniques Malware developers use secure deletion, data hiding, and obfuscation

XVII. FUTURE RESEARCH DIRECTIONS

AI-driven Forensics

Machine learning can automate artifact classification, anomaly detection, and malware attribution. Research is progressing in training models on forensic datasets to improve speed and accuracy.

Blockchain for Evidence Integrity

Blockchain provides tamper-evident logging of evidence handling, ensuring chain-of-custody. Several prototypes integrate blockchain with forensic acquisition [14].

IoT and Wearable Device Forensics

Smartwatches, fitness trackers, and connected IoT devices also store critical data. Extending forensic methods to these devices is essential.

Cross-platform and Cloud Forensics

Investigations increasingly involve correlating evidence across devices, apps, and cloud platforms. Hybrid forensic frameworks are needed to unify these sources.

Privacy-preserving Forensics

Balancing evidence extraction with user privacy rights is critical. Techniques such as selective acquisition and privacy-preserving cryptographic methods are gaining traction.

XVIII. CONCLUSION

Mobile devices have transformed digital life but remain highly vulnerable to attacks. From malware and network exploits to social engineering, attackers continuously evolve methods to compromise mobile ecosystems. The real-time statistics presented in Section II demonstrate the escalating threat landscape, with malware incidents and phishing attacks increasing exponentially year-over-year.

Mobile forensics plays an essential role in investigating these threats, supporting law enforcement, and ensuring digital accountability. However, forensic investigations face significant obstacles such as encryption, OS fragmentation, cloud reliance, and privacy constraints. Future solutions lie in combining AI, blockchain, and privacy-preserving frameworks to strengthen forensic processes. By addressing current challenges and embracing innovative technologies, mobile forensics can keep pace with the dynamic threat landscape and provide robust support to legal systems worldwide.

REFERENCES

[1] Statista. (2024). Number of smartphone users worldwide. Statista Global Consumer Survey.

[2] Casey, E. (2011). Digital Evidence and Computer Crime. Academic Press.

[3] Kaspersky. (2025). Attacks on smartphones increased in the first half of 2025. Kaspersky Security Report.

[4] Verizon. (2025). 2025 Mobile Security Index (MSI) Report. Verizon Business.

[5] Zimperium. (2024). 2025 Global Mobile Threat Report. Zimperium Security Research.

[6] Hoog, A. (2011). Android Forensics Investigation, Analysis and Mobile Security for Google Android. Elsevier.

[7] Casey, E. (2011). Digital Evidence and Computer Crime. Academic Press.

[8] Alghafli, H., Clarke, N., & Furnell, S. (2019). Mobile device forensics: A review of tools and approaches. Journal of Digital Forensics, 11(2), 45-68.

[9] Jain, A., & Singh, S. (2021). Security challenges and forensic analysis of mobile devices. International Journal of Computer Applications, 173(5), 12-24.

[10] Chen, Z., Luo, X., & Zhang, Y. (2021). Android kernel exploits and mitigation strategies. ACM Computing Surveys, 53(6), 1-34.

[11] Daryabar, A., Dehghantanha, R., & Choo, K.-K. R. (2017). Forensic investigation of mobile cloud storage services. Computers & Security, 70, 227-244.

[12] National Institute of Standards and Technology (NIST). (2014). Guidelines on mobile device forensics. NIST SP 800-101.

[13] Amnesty International. (2021). Forensic methodology report: How to catch NSO Group's Pegasus. Amnesty International Research.

[14] Al-Khatib, S. O., & Aloul, F. (2020). Blockchain-based evidence management in mobile forensics. IEEE Security & Privacy, 18(5), 20-29.

[15] Patel, B., Kumar, R., & Sharma, A. (2025). A survey on mobile digital forensics: Taxonomy, tools, and techniques. Journal of Forensic Sciences, 70(1), 89-112. https://doi.org/10.1002/spy2.470

[16] Kumar, M., Singh, P., & Verma, S. (2025). Mobile forensics tools for digital crime investigation: A comparative study. International Journal of Information Security and Privacy, 15(2), 34-52.

[17] Almuqren, A. (2024). A systematic literature review on digital forensic techniques for Android smartphones. Science Direct Digital Forensics, 18(3), 201-225. https://doi.org/10.1016/j.difs.2024.08.020

[18] Thompson, L., & Anderson, M. (2024). Forensic analysis of mobile spyware: Security vulnerabilities and detection challenges in Android and iOS. IEEE Transactions on Information Forensics and Security, 19(4), 567-585.

[19] Rahman, K., Hassan, B., & Patel, R. (2024). A blockchain-based malware detection model for IoT and mobile devices. International Journal of Security and Its Applications, 15(1), 42-68. https://doi.org/10.18280/ijsse.150102

[20] Nannan, X., Liu, Y., & Chen, W. (2025). Andro-BCFL: Blockchain and federated learning-based Android malware detection framework. Science Direct Computer Security, 52(7), 445-461. https://doi.org/10.1016/j.cose.2025.01.015

[21] Pardhi, P. R. (2025). Blockchain for decentralized malware detection on Android devices. Journal of Information Systems Technology, 12(2), 78-96.

[22] Johnson, C., Martinez, D., & Lee, S. (2023). Comparative analysis of Android and iOS from security viewpoint. Computer Security Review, 28(5), 112-134. https://doi.org/10.1016/j.csr.2023.10.125

[23] Williams, J., & Brown, K. (2024). Mobile forensics challenges in 2025: Solutions and emerging trends. Digital Forensics Quarterly, 9(3), 201-218.

[24] Sharma, R., Gupta, V., & Singh, A. (2024). Evaluating security vulnerabilities of mobile forensic applications. International Journal of Forensic Science and Forensic Management Systems, 8(1), 55-79.

[25] Anderson, E., Thompson, R., & Foster, M. (2025). Artificial intelligence-driven anomaly detection in mobile forensics. ACM Transactions on Privacy and Security, 28(2), 1-28.

[26] Chen, L., Wang, H., & Liu, X. (2024). Privacy-preserving cryptographic methods for mobile forensic investigations. Journal of Cybersecurity Research, 14(4), 289-310.

[27] Davis, K., & Wilson, S. (2024). IoT and wearable device forensics: Extending investigation methodologies. IEEE Access, 12(8), 95234-95252.

[28] Robinson, P., Green, T., & Adams, M. (2025). Cloud forensics and cross-platform evidence correlation frameworks. International Journal of Digital Investigation, 22(1), 34-52.