International Journal of Multidisciplinary and Innovative Research

ISSN(print): 3050-6883, ISSN(online): 3050-6891

Volume 02 Issue 06 June 2025

DOI: 10.58806/ijmir.2025.v2i6n03

Page No: 178-183

Technical Challenges of Encryption in Mobile Forensics

Mukesh Tiwari[1], Dr. Suman Thapaliya[2]

[1,2]MCS Scholar, Texas International College

ABSTRACT

Mobile device security has advanced rapidly in recent years, creating new challenges for digital forensic investigators. The growing use of sophisticated encryption technologies has particularly transformed how forensic professionals approach evidence extraction and analysis. This seminar paper examines the technical challenges posed by encryption in mobile forensics, focusing on Full Disk Encryption (FDE), File-Based Encryption (FBE), and hardware-backed security modules such as Android Keystore and Apple Secure Enclave. The objectives include evaluating current encryption technologies, analyzing their impact on forensic data extraction, and assessing the effectiveness of standard forensic tools. The methodology is based on a literature review and comparative analysis of encryption standards and forensic techniques. Key findings reveal that modern encryption methods create substantial barriers for forensic practitioners, necessitating innovative approaches that balance lawful access and user privacy. The paper concludes with recommendations for the digital forensics' community and suggestions for future research.

KEYWORDS: Mobile Forensics; Digital Evidence; Encryption; Android Security; iOS Security

ARTICLE DETAILS

Published On:
16 June 2025

Available on:
https://ijmir.com

1. INTRODUCTION

1.1 Background and Context

In modern criminal investigations, mobile devices are seized at nearly every crime scene, and their data forms a critical part of the evidence (Fukami et al., 2021) and their extensive digital footprints, from geolocation logs to encrypted communications, provide essential intelligence for resolving investigations in today's interconnected environment (Tamma et al., 2021). The significance of mobile devices in criminal investigations has elevated the importance of mobile forensics, the science of acquiring and analyzing data from mobile devices. However, as manufacturers implement robust encryption technologies, forensic analysts face increasing challenges in data extraction and analysis.

1.2 Relevance in Computer Science

The intersection of cybersecurity, cryptography, and digital forensics represents a vital and evolving area within contemporary computer science (Tamboli, 2024). Encryption technologies, although indispensable for protecting user privacy and securing digital data, simultaneously complicate lawful forensic access. This creates an ongoing tension between the need for robust security and the demands of criminal investigations, posing a significant challenge for both researchers and practitioners in the field.

1.3 Problem Statement

As mobile operating systems increasingly adopt advanced encryption methods like Full Disk Encryption (FDE), File-Based Encryption (FBE), and hardware-backed secure environments, retrieving data during forensic investigations has become more challenging. While these security measures are crucial for protecting user privacy, they can also hinder law enforcement from accessing digital evidence that may be vital to solving criminal cases.

1.4 Objectives and Scope

This seminar paper is guided by the following objectives:

- Evaluate current encryption technologies implemented in modern mobile devices.
- Analyze how encryption impacts the process of forensic data extraction.
- Assess the effectiveness of commonly used forensic tools and propose evidence-based solutions.
- Focus specifically on the Android and iOS platforms, which dominate the mobile device landscape.

1.5 Organization of the Paper

The structure of this paper is organized into five main sections. Section 2 presents a review of the relevant literature, focusing on encryption in mobile forensics. Section 3 explains the methodology used for this study. Section 4 provides analysis and discussion of key findings. Finally, Section 5 concludes the paper with recommendations and directions for future research.

2. LITERATURE REVIEW

2.1 Digital Forensics and Mobile Forensics

Digital forensics is defined as the application of scientific methods to the identification, collection, examination, and analysis of digital data, ensuring integrity and legal admissibility (Kent (NIST) et al., 2006). Mobile forensics, a specialized branch, addresses the unique challenges of extracting evidence from smartphones and tablets, which store sensitive personal and transactional data (Tamma et al., 2021).

2.2 Evolution of Encryption in Mobile Devices

Modern mobile platforms integrate robust, multi-layered security mechanisms designed to safeguard user data and privacy (Tamma et al., 2021). While these features enhance protection against unauthorized access, they also create significant barriers for forensic practitioners during acquisition and analysis.

Mobile devices now typically include default encryption layers that span both hardware and software, complicating direct access to stored data (Zinkus et al., 2021). Forensic access often requires overcoming these encryption barriers, which may not always be feasible through standard means. A prominent example of such challenges is the FBI versus Apple case, where Apple's robust security architecture prevented authorities from accessing data on an iPhone used by a suspect in the San Bernardino attack (Ahlam, 2020). This incident highlighted the tension between data security and lawful forensic access, reinforcing the need for innovative solutions that balance privacy with investigative requirements (Schulze, 2017).

2.3 Evolution of Mobile Encryption Standards

Modern mobile operating systems rely on encryption as a foundational mechanism for protecting user data (Akhtar, 2024). By transforming plaintext into ciphertext, these systems ensure that data at rest cannot be read without the correct cryptographic keys. While these protections are essential for user privacy, they introduce significant obstacles for forensic practitioners by restricting access to critical evidence. This section examines how encryption is implemented on the two dominant mobile platforms, Android and iOS, and highlights the challenges each poses to established forensic workflows.

2.4 Android Encryption

2.4.1 Full-Disk Encryption (FDE)

Full-Disk Encryption (FDE) on Android devices encodes all user data with an encryption key, automatically encrypting data before storage and decrypting it on access. According to Tamma et al., (2021), starting with Android 6.0 Marshmallow, Google mandated FDE for most devices meeting hardware standards. In the FDE encryption key is protected by the user's PIN, pattern, or password, making data access dependent on these credentials (Tamma et al., 2021). This security mechanism, while critical for user privacy, creates substantial forensic acquisition barriers. FDE typically employs AES-128 or higher encryption, with cryptographic keys derived directly from the user's lock screen input, thereby reinforcing the complexity of bypassing such protections in a forensic context (Samsung Knox, 2024).

While FDE secures entire storage partitions, Android's shift to File-Based Encryption (FBE) in later versions introduced granular security controls and new forensic complexities.

2.4.2 File-Based Encryption (FBE)

FBE represents a paradigm shift in Android's security architecture, introduced in Android 7.0 and higher to address limitations of Full-Disk Encryption (FDE) (Fukami et al., 2021). Unlike FDE, which encrypts entire storage partitions, FBE allows different files to be encrypted with different keys that can be unlocked independently (Tamma et al., 2021). In FBE, each file is independently encrypted using AES-256, with a unique File Encryption Key that is derived from a Primary Key (Samsung Knox, 2024). File-Based Encryption enables more granular control compared to Full-Disk Encryption, though it introduces forensic complications.

2.4.3 Android Keystore and Trusted Execution Environment (TEE)

Android devices include a Keystore system that provides a secure container for cryptographic keys. Keys generated or imported into the Keystore can be used to perform cryptographic operations, but cannot be extracted in plaintext from the Keystore (Tamma et al., 2021). Hardware-backed Keystores provides security at the hardware level. As a result, even if the main operating system is compromised, the keys remain protected against extraction or tampering (Tamma et al., 2021).

A Trusted Execution Environment (TEE) is a hardware-isolated processor or subsystem designed to execute security-sensitive code and protect secret data (such as cryptographic keys) from the main, untrusted operating system (Hoang et al., 2022). The TEE maintains its own secure boot chain, enforces integrity checks on loaded code, and provides a controlled API for the normal OS to request cryptographic operations without exposing keys (Hoang et al., 2022).

While Android's encryption mechanisms complicate forensic workflows, iOS devices present their own unique challenges through hardware-backed security architectures like the Secure Enclave.

2.5 iOS Encryption

On iOS devices, beginning with the iPhone 4, the entire filesystem is secured by a Filesystem Key computed from the device's unique hardware key (UID) and retained in effaceable storage, an isolated area between the hardware and OS layers (Tamma et al., 2021). Because this key never leaves secure storage, any raw dump (e.g., via JTAG or Chip-Off) contains only ciphertext, rendering these acquisition methods ineffective without first unlocking the device or exploiting a vulnerability (Tamma et al., 2021)

2.5.1 Data Protection & Key Hierarchy

Every file in the iOS filesystem is encrypted with a unique AES 256-bit key, wrapped with a class key and then encrypted under the filesystem key (Edge & Trouton, 2023). These class keys are protected by the device's unique identifier (UID) and, in certain scenarios, the user's passcode. These class-based protections significantly affect the ability of forensic analysts to access encrypted data, especially when devices remain locked or unexploited (Zinkus et al., 2021).

Keybags, which store class keys across operational contexts such as user access, device use, backup and iCloud are secured within the Secure Enclave on A9 and newer chips (Zinkus et al., 2021). This hardware component uses passcode-based key derivation (PBKDF2 with UID) and anti-replay mechanisms to resist brute force attacks, making unauthorized access extremely difficult (Apple Inc., 2024; Zinkus et al., 2021).

2. 6 Research Gaps

Many recent studies have pointed out that accessing encrypted data on modern mobile devices is becoming more and more difficult (Fukami et al., 2021). This is largely because of hardware-backed security like Secure Enclave in iOS or the Trusted Execution Environment on Android (Fukami et al., 2021; Tamma et al., 2021). These features are specifically designed to isolate and protect cryptographic keys, which makes standard forensic methods much less effective. Moreover, frequent updates to mobile operating systems often bring new encryption methods and security features, making it increasingly difficult for forensic tools to keep pace and remain effective. While these advancements are great for user privacy, they create major problems for forensic investigators. There's a clear need for new techniques that can handle these technical barriers but still ensure that the evidence remains valid in court. Although the challenges are well recognized, there's still a lack of solid research or practical frameworks to guide forensic practitioners through these obstacles, which opens a clear path for further work in this area.

3. METHODOLOGY

This seminar paper is based on a literature review approach. It draws from peer-reviewed articles, technical documentation, and reports from industry-leading sources to explore encryption mechanisms and forensic practices. A comparative analysis is used to examine how these technologies function across the Android and iOS platforms, focusing on their impact on data accessibility during forensic investigations. Due to certain institutional limitations, the study does not involve hands-on testing of forensic tools. Instead, it relies on well-documented methodologies, previously published case studies, and publicly available forensic research to support its findings.

4. ANALYSIS AND DISCUSSION

4.1 Impact of Encryption Mechanisms

- Android: FDE and FBE ensure that data at rest is inaccessible without user credentials (Gasser & Aad, 2023). Hardware-backed Keystore and Trusted Execution Environment (TEE) further isolate cryptographic keys, making extraction via physical methods (e.g., JTAG, Chip-Off) largely ineffective without device unlock (Tamma et al., 2021)
- iOS: The Secure Enclave and hierarchical keybags protect per-file keys, requiring interaction with secure hardware for decryption. Physical acquisition methods yield only ciphertext unless the device is unlocked (Tamma et al., 2021).
- Other notable Operating Systems: While Android and iOS dominate the mobile ecosystem, alternative platforms such as Harmony OS developed by Huawei, present distinct forensic challenges (Abdul Kadir et al., 2024). Harmony OS employs multi-layered security features including Trusted Execution Environments (TEEs), posing challenges similar to those found in high-end Android devices (Jia et al., 2024). Based on practical experience in forensic investigations, platforms like KaiOS currently hold limited relevance in digital forensics due to their comparatively weak encryption architecture, minimal user data footprint, and lack of compatibility with mainstream forensic acquisition tools.

These encryption strategies, while essential for protecting user privacy, significantly limit the ability of investigators to recover usable evidence from mobile devices.

4.2 Effectiveness of Forensic Tools

Traditional forensic acquisition methods, such as physical acquisition, JTAG, and Chip-Off, are still used to extract raw memory or storage data from mobile devices (Da Costa et al., 2022). However, with the increasing use of hardware-backed encryption, their effectiveness has become extremely limited. Even when a memory dump is obtained, the contents are typically encrypted and unreadable without access to the cryptographic keys stored in secure hardware environments like the Secure Enclave (iOS) or Trusted Execution Environment (Android) (Tamma et al., 2021).

In real-world practice, we've found that if a high-end Android or iOS device is locked, it is nearly impossible to extract usable data without access to premium forensic solutions such as Cellebrite UFED Premium or Magnet GrayKey. These tools are designed to handle locked and encrypted devices, but they are not always available due to licensing costs or institutional limitations. As a result, many investigations involving modern smartphones face significant delays or reach a dead end when such tools are not accessible.

While forensic software continues to improve, its success against encryption often depends on the specific device model, Chipset, OS version, and whether the device is unlocked. In cases where those conditions are not met, even the most advanced tools may offer little to no access to user data, highlighting a major limitation in current mobile forensic capabilities.

4.3 Technical and Legal Challenges

Mobile forensic investigations today face both technical and legal hurdles that are difficult to overcome (Fakhouri et al., 2024). One of the biggest technical barriers is the dependence on user credentials. Most encryption schemes are tied directly to a passcode, pattern, or biometric input, without which data remains inaccessible. Even if a physical image of the device is obtained, decryption is not possible without the associated credentials. Modern mobile devices implement layered encryption key hierarchies, where each key is wrapped in multiple cryptographic layers (Apple Inc., 2024). This architecture significantly complicates forensic decryption efforts, even when partial access to the device is possible (Zinkus et al., 2021).

Another major challenge lies in the hardware-level protections. Secure modules like Apple's Secure Enclave or Android's Trusted Execution Environment (TEE) isolate critical cryptographic keys from the main system (Zinkus et al., 2021). These hardware-backed components are designed to resist both software-based attacks and invasive hardware techniques like Chip-Off, effectively blocking many traditional forensic approaches (Zinkus et al., 2021).

From a legal standpoint, any method adopted for data acquisition must comply with applicable laws and procedural safeguards. This is essential to ensure that the extracted digital evidence remains admissible in a court of law and is not challenged on the grounds of unlawful or unethical collection.

4.4 Survey Insights

To support this study, a survey was conducted among 30 digital forensic professionals, using 20 Likert-scale statements to capture views on encryption challenges, tool effectiveness, and legal considerations. Responses were rated from 1 (Strongly Disagree) to 5 (Strongly Agree).

The results showed strong agreement on key issues. Participants widely acknowledged the challenges of encryption, especially the impact of FDE and FBE on Android and iOS devices, and the limitations faced when advanced tools like UFED Premium or Magnet GrayKey are unavailable, both statements averaging 4.75. Ethical concerns were also evident, with most agreeing that exploit-based methods must follow legal safeguards.

One clear disagreement emerged regarding open-source tools. Over 87% respondents disagreed that open-source tools are as effective as commercial ones, showing a preference for industry-grade solutions in complex mobile forensic cases.

Overall, the survey reinforced the paper's findings: encryption continues to be a serious obstacle in mobile forensics, and access to the right tools and legal clarity remains essential for effective investigations.

5. CONCLUSION AND FUTURE WORK

5.1 Summary of Findings

The study highlights that modern encryption methods such as Full-Disk Encryption (FDE), File-Based Encryption (FBE), and hardware-backed security modules pose major challenges to mobile forensic investigations. As these technologies continue to evolve, traditional acquisition methods are becoming less effective. Forensic access is now heavily dependent on user credentials and secure hardware environments, which are often resistant to both physical and software-based extraction. These findings underscore the growing need for innovative solutions that can support lawful access to digital evidence while still respecting user privacy and legal standards.

5.2 Limitations

This study is based entirely on a review of existing literature, technical documentation, and survey feedback. It does not include empirical tool testing or access to proprietary forensic data.\

5.3 Recommendations and Future Research

- Foster collaboration with device manufacturers to develop lawful access mechanisms that respect both privacy and investigative needs. These partnerships could help strike a balance between security design and forensic accessibility.
- Encourage further research into ethical vulnerability exploitation and secure methods for credential recovery. This includes exploring how such techniques can be applied responsibly within legal frameworks.
- Establish standardized procedures for handling encrypted digital evidence to ensure consistency, admissibility in court, and compliance with legal protocols.
- Explore the potential of emerging technologies, such as artificial intelligence and quantum computing, to advance mobile forensic capabilities and address encryption challenges more effectively.

5.4 Conclusion

Mobile encryption has made digital investigations more complex than ever. While these security measures are important for protecting user data, they also create serious roadblocks for forensic examiners, especially when it comes to accessing locked devices. This paper explored how encryption techniques like Full-Disk Encryption, File-Based Encryption, and hardware-based modules such as Secure Enclave and TEE make it harder to extract usable evidence.

Based on the literature reviewed and the feedback collected from professionals in the field, it's clear that current forensic tools and methods aren't always enough to deal with these challenges. Investigators often face situations where even basic access to data isn't possible without high-end forensic solutions or services such as Cellebrite Advanced Services (CAS), which offer specialized forensic support.

Looking ahead, there's a clear need for better collaboration, updated protocols, and responsible research into new solutions. At the same time, any approach must respect legal boundaries and privacy rights. For mobile forensics to remain effective, it needs to keep pace with fast-moving changes in technology without compromising the ethical standards on which the field depends on.

REFERENCES

1) Abdul Kadir, A. F., Habibi Lashkari, A., & Daghmehchi Firoozjaei, M. (2024). Other operating systems. In Understanding cybersecurity on smartphones: : Challenges, Strategies, and Trends (pp. 71-87). Cham: Springer. https://doi.org/10.1007/978-3-031-48865-8_5
2) Ahlam, R. (2020). Apple, the government, and you: Security and privacy implications of the global encryption debate. Fordham International Law Journal, 44, 771. Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/frdint44&div=27&id=&page=
3) Akhtar, Z. B. (2024). Securing operating systems (OS): A comprehensive approach to security with best practices and techniques. International Journal of Advanced Network, Monitoring and Controls, 9(1). https://doi.org/10.2478/ijanmc-2024-0010
4) Apple Inc. (2024). Apple platform security guide (December 2024). Retrieved from https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf
5) Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd ed.). Academic Press.
6) Da Costa, A. M., De Sà, A. O., & Machado, R. C. (2022). Data acquisition and extraction on mobile devices—A review. In 2022 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0 & IoT) (pp. 294–299). IEEE. https://doi.org/10.1109/MetroInd4.0IoT54413.2022.9831724
7) Digital Forensic Research Workshop. (2001). A road map for digital forensic research (US-01). Retrieved from https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf
8) Edge, C., & Trouton, R. (2023). Endpoint Encryption. In Apple Device Management: A Unified Theory of Managing Macs, iPads, iPhones, and Apple TVs. Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4842-9156-6_7
9) Fakhouri, H. N., AlSharaiah, M. A., Alkalaileh, M., & & Dweikat, F. F. (2024). Overview of challenges faced by digital forensic. In 2024 2nd International Conference on Cyber Resilience (ICCR) (pp. 1–8). IEEE. https://doi.org/ieeexplore.ieee.org/abstract/document/10532850
10) Fortinet. (n.d.). What Is Encryption? Retrieved May 31, 2025, from https://www.fortinet.com/resources/cyberglossary/encryption
11) Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. Forensic Science International: Digital Investigation, 38. https://doi.org/10.1016/j.fsidi.2021.301169
12) Gasser, L., & Aad, I. (2023). Trends in Data Protection and Encryption Technologies. Springer. https://doi.org/10.1007/978-3-031-33386-6

13) Hoang, T. T., Duran, C., Serrano, R., Sarmiento, M., Nguyen, K. D., Tsukamoto, A., & Pham, C. K. (2022). Trusted execution environment hardware by isolated heterogeneous architecture for key scheduling. IEEE Access, 10, 46014–46027. https://doi.org/10.1109/ACCESS.2022.3169618
14) Jia, S., Wang, X., Song, M., & Chen, G. (2024). Agent Centric Operating System – a comprehensive review and outlook for operating system. arXiv. https://doi.org/10.48550/arXiv.2411.17710
15) Kent (NIST), K., Chevalier (BAH), S., Grance (NIST), T., & Dang (BAH), H. (2006). Guide to Integrating Forensic Techniques into Incident Response. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86
16) Oettinger, W. (2022). Learn computer forensics: Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence (2nd ed.). Packt.
17) Samsung Knox. (2024, February 20). File-based encryption (FBE) and full-disk encryption (FDE). Retrieved May 31, 2025, from Samsung Knox Documentation: https://docs.samsungknox.com/admin/knox-platform-for-enterprise/kbas/kba-360039577713/#What
18) Schulze, M. (2017). Clipper meets Apple vs. FBI: A comparison of the cryptography discourses from 1993 and 2016. Media and Communication, 5(1). https://doi.org/10.17645/mac.v5i1.805
19) Tamboli, M. (2024). Forensic Encryption: Discovering Hidden Digital Secrets. ZTTTkkS Open Access / Stechnolock. Retrieved from https://www.stechnolock.com/article/Forensic-Encryption-Discovering.pdf
20) Tamma, R., Skulkin, O., Mahalik, H., & Bommisetty, S. (2021). Forensically investigate and analyze iOS, Android, and Windows 10 devices. Packt.
21) Tiepolo, G. (2022). iOS Forensics for Investigators: Take mobile forensics to the next level by analyzing,. Packt.
22) Zinkus, M., Jois, T. M., & Green, M. (2021). Data security on mobile devices: Current state of the art, open problems, and proposed solutions. https://doi.org/10.48550/arXiv.2105.12613