IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 11 ISSUE : 03 Print / Issue Publication Date: July 2026

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2026.v11i03.013

Indexed In

Google SCHOLAR · OPEN ACCESS · doi · Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 83-89
Published Online July 2026 in IJEAST (http://www.ijeast.com)

AN ANALYTICAL STUDY OF CHALLENGES IN MOBILE FORENSIC INVESTIGATION OF ENCRYPTED ANDROID DEVICES

Pandule A. B., More S.J., Gore R.P., Deshmukh P.A., Pawade V.S., Joshi D.C. and Thakare V.J.
Cyber Crime, Tape and Speaker Identification Department,
Regional Forensic Science Laboratory, Pune,
Home Department, Maharashtra State, India

Abstract: **Modern Android operating systems have widely adopted encryption mechanisms, which has changed mobile forensic investigations drastically. Although encryption improves user privacy and data security, it has become a major challenge to law enforcement agencies and forensic practitioners during evidence acquisition and analysis. This article identifies the issues that are faced by the mobile forensics due to full disk encryption, file-based encryption, secure hardware backed key storage and the Android security architectures changes. It shows the limitations encountered during logical, file system, and physical acquisition methods on encrypted Android devices. Moreover, the research talks about the obstacles in law, technology, and procedures that affect forensic investigations. The article intends to equip forensic professionals with a thorough knowledge of the present encryption, related issues and the possible ways in which research can be communicated, and tools can be developed in mobile forensics. While the technical findings are globally applicable, investigative workflows are analyzed using the Indian forensic ecosystem as a representative case study.**

Keywords: **Mobile Forensics, Android Encryption, File-Based Encryption, Digital Evidence, Cybercrime Investigation, Mobile Security**

I. INTRODUCTION

The rapid digital transformation in India has led to widespread adoption of smartphones for communication, online banking, digital payments, e-governance services, and social media interaction. Initiatives such as Digital India and the growth of Unified Payments Interface have further increased dependence on mobile devices for daily activities. Consequently, smartphones have become a primary repository of digital evidence in a wide range of cybercrime investigations, including financial fraud, identity theft, cyberstalking, and organized cyber offenses [4], [7].

Among available mobile platforms, Android devices account for a significant majority of smartphones used in India. Due to their affordability and wide manufacturer support, Android devices are commonly encountered during digital forensic examinations conducted by law enforcement agencies and forensic laboratories. As a result, effective forensic analysis of Android devices is crucial for timely and accurate cybercrime investigations [2], [4].

In parallel with increased smartphone usage, Android operating systems have undergone substantial security enhancements aimed at protecting user data. Earlier Android versions permitted relatively easier access to stored data using conventional forensic acquisition techniques. However, the introduction of full disk encryption (FDE), followed by file-based encryption (FBE), has significantly transformed the mobile forensic landscape. These encryption mechanisms ensure that user data remains inaccessible without proper authentication, even when physical access to the device is obtained [2], [6].

While encryption is essential for safeguarding user privacy and aligning with modern data protection principles, it creates significant challenges for forensic investigators. Investigators frequently encounter encrypted devices where access to critical artefacts is restricted due to unknown credentials, hardware-backed key storage, or secure boot enforcement. In many cases, only partial data extraction is possible, which can affect the completeness of forensic analysis and the reconstruction of events [6], [4].

Additionally, mobile forensic investigations in India must operate within a defined legal framework that balances investigative requirements with constitutional protections of privacy. Judicial scrutiny regarding the admissibility, integrity, and legality of digital evidence further emphasizes the need for standardized and legally sound forensic methodologies. [1][4][6]

This paper aims to analyze the challenges associated with mobile forensic investigations of encrypted Android devices, with specific reference to the Indian investigative scenario. By examining technical, procedural, and legal limitations, the study seeks to highlight gaps in current forensic practices and identify areas for future research and capability enhancement in mobile forensics.

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 83-89
Published Online July 2026 in IJEAST (http://www.ijeast.com)

II. RESEARCH METHODOLOGY

This study adopts a qualitative analytical methodology based on three complementary approaches: (i) a systematic literature review, (ii) technical analysis of Android security architecture, and (iii) examination of investigative practices and applicable legal frameworks.

The literature review incorporates peer-reviewed journal articles, conference proceedings, technical standards, and official Android documentation published between 2015 and 2024. Sources were collected from platforms such as IEEE Xplore, Digital Investigation, Forensic Science International: Digital Investigation, and official Android security documentation. Foundational and review-based studies in mobile forensics were primarily referred to for establishing the research context and identifying key challenges in the field [4], while standardized forensic guidelines were used to ensure methodological reliability and alignment with accepted practices [6].

The technical analysis focuses on Android security mechanisms, including Full Disk Encryption (FDE), File-Based Encryption (FBE), hardware-backed keystore, Trusted Execution Environment (TEE), secure boot, and access control enforcement, to evaluate their impact on forensic acquisition and analysis. These mechanisms are examined based on official Android security architecture and forensic best practice guidelines [2],[6].

Practical insights are derived from commonly followed investigative workflows in forensic laboratories, particularly in the Indian context. This includes evidence acquisition under Before First Unlock (BFU) and After First Unlock (AFU) conditions, adherence to procedural requirements, and considerations related to the admissibility and integrity of digital evidence. These practices are aligned with established mobile forensic guidelines and frameworks [6].

III. EVOLUTION OF ENCRYPTION IN ANDROID DEVICES AND ITS IMPACT ON INVESTIGATIVE PRACTICE IN INDIA

The security architecture of Android has evolved significantly across successive versions, with a strong emphasis on protecting user data through advanced encryption mechanisms[13]. This evolution has had a direct impact on mobile forensic methodologies and investigative workflows adopted by law enforcement agencies, particularly in data acquisition and accessibility challenges [2], [6].

A. Full Disk Encryption in Early Android Versions

Full Disk Encryption (FDE) was introduced in Android to secure user data by encrypting the entire data partition using a single encryption key derived from user credentials. In earlier Android versions, forensic acquisition was relatively feasible once the device was unlocked or when vulnerabilities could be leveraged during the boot process. From an investigative standpoint, FDE-based devices allowed forensic laboratories to achieve broader access to stored data, often enabling physical or file system extraction under controlled environments [3], [4].

However, even during the FDE phase, investigators faced limitations when devices were seized in a powered-off or locked condition. Access to encrypted partitions remained dependent on successful authentication, highlighting the critical importance of device state at the time of seizure [6].

B. Transition to File-Based Encryption

Android later transitioned from FDE to File-Based Encryption (FBE), introducing a more granular and secure encryption framework. Under FBE, individual files are encrypted using distinct keys, and access to data is governed by two operational states: Before First Unlock (BFU) and After First Unlock (AFU). This transition significantly enhanced data protection while simultaneously complicating forensic acquisition processes [2], [6].

This architectural shift has substantially influenced mobile forensic practices. In the BFU state, only limited system-level and device-encrypted data is accessible, whereas the majority of user data remains protected until authentication. In contrast, the AFU state permits broader access to credential-encrypted data once the device has been unlocked after boot, thereby providing improved but still controlled forensic visibility [6].

C. BFU and AFU States in Indian Investigative Scenarios

In practical investigative scenarios in India, Android devices are often seized during raids, arrests, or complaint-based actions in a locked or powered-off condition. Consequently, investigators frequently encounter devices in the BFU state, where access to critical artefacts such as application data, communication records, and user-generated content is significantly restricted [6].

When devices are obtained in the AFU state—typically when seized while powered on or recently unlocked—investigators may gain limited access to decrypted or volatile data. However, maintaining this state requires strict adherence to evidence handling procedures, as rebooting or power interruption can revert the device to BFU, resulting in immediate loss of access to protected data [6].

Operational challenges such as delayed device submission, unavailability of user credentials, and legal constraints on compelled unlocking further increase the likelihood of BFU-state examinations. These factors reduce the scope of recoverable evidence and may extend investigation timelines in forensic laboratories [4], [6].

D. Hardware-Backed Key Storage and Secure Execution Environments

Modern Android devices increasingly implement hardware-backed key storage using Trusted Execution Environments

(TEE) or secure hardware elements. In this architecture, encryption keys are generated and stored within isolated secure environments and are not accessible to the main operating system. This significantly enhances data protection and prevents key extraction, even when physical access to the device is available [2], [6].

From a forensic perspective, such hardware-level security mechanisms impose substantial limitations on traditional acquisition techniques. Software-based bypass methods are largely ineffective, necessitating reliance on lawful procedures, partial data extraction, or alternative evidence sources during investigations [6].

E. Implications for Mobile Forensic Methodologies

The evolution of Android encryption has compelled forensic investigators to adapt their methodologies. Increased emphasis is placed on factors such as timing of device seizure, preservation of device state, proper documentation of BFU and AFU conditions, and correlation with external data sources including cloud storage, network logs, and service provider records [4],[6].

A clear understanding of BFU and AFU states is essential for accurately interpreting extracted data and recognizing its limitations. Failure to account for these states may lead to incorrect assumptions regarding data availability or misinterpretation of forensic findings.

IV. MOBILE FORENSIC ACQUISITION METHODS AND ENCRYPTION CONSTRAINTS

Mobile forensic investigations rely on multiple acquisition techniques to extract digital evidence from devices. The effectiveness of these techniques is significantly influenced by encryption mechanisms implemented in modern Android systems. In practical investigative environments, particularly in India, where devices are often obtained without user credentials and under strict legal, ethical, and procedural requirements, encryption imposes substantial limitations on data accessibility [6], [8].

A. Logical Acquisition

Logical acquisition involves extracting data through the device's operating system using standard application programming interfaces. This method typically retrieves user-accessible artefacts such as contacts, call logs, messages, and limited application data [4][9].

On encrypted Android devices, logical acquisition is significantly restricted, especially when the device is in the Before First Unlock (BFU) state. Most user data remains encrypted and inaccessible without authentication. In many investigative scenarios, where credentials are unavailable due to non-cooperation or legal limitations, logical acquisition often yields minimal evidentiary value and is primarily useful for preliminary analysis [6].

B. File System Acquisition

File system acquisition aims to obtain a structured copy of the device's file system, enabling analysis of directories, databases, and configuration files. Prior to advanced encryption mechanisms, this method provided comprehensive insights into user activity and application behavior [3], [4][9].

With the adoption of File-Based Encryption (FBE), access to file system data is largely dependent on the device being in the After First Unlock (AFU) state. In practical scenarios, maintaining the AFU state during seizure, transport, and examination is challenging due to power constraints, procedural handling, and delays. Any reboot or power loss reverts the device to BFU, thereby restricting access to encrypted user data [6].

Consequently, file system acquisition on modern encrypted devices often results in partial datasets, requiring careful interpretation and explicit documentation of encryption-related limitations in forensic reports.

C. Physical Acquisition

Physical acquisition involves capturing a bit-by-bit image of the device's storage. Traditionally, this method provided the most comprehensive data access, including deleted artefacts and unallocated space [3][9][10].

However, modern Android encryption has significantly reduced its effectiveness. Even when raw storage data is acquired, it remains encrypted and unreadable without access to encryption keys, which are protected within secure hardware environments. Additionally, forensic practices must adhere to legal and procedural standards that limit invasive techniques and emphasize data integrity [2], [6][9].

As a result, physical acquisition increasingly serves as a method for evidence preservation rather than direct data interpretation in encrypted environments.

D. Live Forensic Acquisition

Live forensic acquisition refers to data collection while the device is powered on and operational. This approach can provide access to volatile memory, running processes, and decrypted data when the device is in the AFU state [6].

In real-world investigations, opportunities for live acquisition are limited and must be carefully managed to ensure forensic integrity and legal admissibility. Improper handling may alter system data or compromise evidentiary value. Furthermore, live acquisition requires trained personnel and immediate response, which may not always be feasible in field conditions.

Despite these constraints, live acquisition remains valuable when devices are seized in an unlocked or recently unlocked state, provided strict procedural safeguards are followed.

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 03, ISSN No. 2455-2143, Pages 83-89
Published Online July 2026 in IJEAST (http://www.ijeast.com)

E. Summary of Encryption Constraints on Acquisition Methods

The effectiveness of mobile forensic acquisition techniques is increasingly dependent on the encryption state of the device. In practice, investigators must adapt to these constraints by combining multiple methods and clearly documenting the scope and limitations of acquired data [1].

In the Indian investigative context, encryption necessitates a shift from reliance on single-device extraction toward a multi-source evidence approach. Investigators must correlate device data with external sources such as cloud storage, service provider records, and network logs to reconstruct events comprehensively [4], [6].

Table I summarizes the impact of Android encryption on commonly used forensic acquisition methods and highlights practical limitations encountered during investigations.

Acquisition Method	Data Accessibility	Effect of Encryption	Practical Observations in Indian Investigations
Logical Acquisition	Limited user-level data	Majority of user data inaccessible in BFU state; requires authentication	Often yields minimal artefacts due to lack of credentials and legal constraints
File System Acquisition	Partial file system access	Access dependent on AFU state; encrypted user files remain protected	AFU state difficult to maintain during seizure and transport
Physical Acquisition	Raw storage image	Encrypted data remains unreadable without hardware-backed keys	Useful mainly for evidence preservation, not direct analysis
Live Acquisition	Volatile and decrypted data	Requires device to be powered on and unlocked	Limited field feasibility; strict procedural safeguards required

Table I summarizes the impact of Android encryption on commonly used mobile forensic acquisition methods and highlights practical limitations encountered during investigations.

The table illustrates that encryption significantly reduces the effectiveness of traditional acquisition methods. Logical acquisition provides limited visibility, file system extraction is conditional on device state, and physical acquisition no longer guarantees access to usable data. These limitations directly affect evidence completeness, timeline reconstruction, and the overall reliability of forensic findings [6].

V. KEY CHALLENGES IN MOBILE FORENSICS WITH ENCRYPTED ANDROID DEVICES

The implementation of advanced encryption mechanisms in modern Android devices has introduced significant challenges for mobile forensic investigations. These challenges extend beyond technical barriers to include procedural and legal complexities. In investigative environments such as India, where timely access to digital evidence is critical and legal safeguards are stringent, encryption substantially affects the scope, efficiency, and reliability of forensic analysis [4], [6].

A. Full Disk and File-Based Encryption Barriers

The transition from Full Disk Encryption (FDE) to File-Based Encryption (FBE) has fundamentally changed how data is accessed on Android devices. Under FBE, the majority of user data remains protected until successful authentication, restricting access in the Before First Unlock (BFU) state. Since many devices are seized in locked or powered-off conditions, investigators frequently encounter encrypted datasets that cannot be accessed without credentials [2], [6].

In practical scenarios, delays in device submission and limited opportunities for live examination further intensify this challenge. Consequently, critical artefacts such as communication records, application databases, and user-generated content often remain inaccessible, impacting evidentiary completeness [6].

B. Secure Boot and Verified Boot Mechanisms

Modern Android devices implement secure boot and verified boot mechanisms to ensure system integrity and prevent unauthorized modifications. These protections restrict the loading of untrusted firmware and maintain a trusted execution chain [2].

From a forensic standpoint, secure boot limits the ability to perform low-level access or custom boot-based analysis. In legally sensitive environments, adherence to non-invasive and defensible procedures further restricts such approaches, as any system alteration may raise concerns regarding evidence integrity and admissibility [6][11].

C. Hardware-Backed Key Storage and Secure Execution Environments

Contemporary Android devices increasingly utilize hardware-backed key storage through Trusted Execution Environments (TEE) or secure elements. Encryption keys are generated and stored within isolated hardware components, making them inaccessible to conventional software-based extraction techniques [2], [6].

This design presents a major challenge for forensic investigators, as physical possession of the device alone does not guarantee access to encrypted data. In many investigative scenarios, the absence of user credentials results in persistent data inaccessibility, even after extensive forensic attempts [6].

D. Application-Level Encryption and Secure Applications

In addition to system-level encryption, many Android applications implement their own security mechanisms, including encrypted local storage and end-to-end encryption. Communication and financial applications frequently protect data using multiple layers of encryption[12].

This significantly limits forensic analysis, as even when partial file system access is available, application-level artefacts may remain encrypted. As a result, investigators may only retrieve metadata rather than meaningful content, reducing the evidentiary value of extracted data [4], [6].

E. Limitations of Forensic Tools and Standardization

Mobile forensic tools often struggle to keep pace with rapid changes in Android security architecture. Their effectiveness varies depending on device models, operating system versions, and security patch levels [4].

Operational environments may also face constraints related to resources, tool availability, and technical expertise. These factors can result in inconsistent extraction outcomes across devices, creating challenges in maintaining standardized forensic procedures and consistent evidence interpretation [4], [6].

F. Legal and Procedural Constraints

Mobile forensic investigations must operate within established legal frameworks that protect individual privacy while enabling lawful evidence collection. Issues such as consent, lawful access, and proper documentation directly influence the admissibility of digital evidence[6], [8], [9].

Encryption further complicates this balance by restricting access even when devices are lawfully seized. Investigators must ensure transparent reporting of limitations, maintain procedural integrity, and avoid techniques that could compromise legal validity. These constraints often require reliance on supplementary sources such as cloud data and service provider records [6].

G. Impact on Investigation Timelines and Case Outcomes

The combined impact of encryption-related challenges often leads to extended investigation timelines. Delays in data acquisition, partial evidence availability, and dependence on alternative data sources can slow down case progression.

In high-volume cybercrime environments, such delays increase the workload on forensic laboratories and investigating agencies. Limited access to critical mobile data may also influence case outcomes, underscoring the need for adaptive forensic strategies, improved technical capabilities, and supportive policy frameworks [4], [6].

VI. DISCUSSIONS

The findings of this study demonstrate that encryption in modern Android devices is no longer a standalone technical feature but a fundamental component shaping the entire mobile forensic investigation process. In the context of India, where Android devices dominate the mobile ecosystem and cybercrime cases are increasing, encryption significantly affects investigative efficiency, evidence accessibility, and overall case outcomes [4], [6].

One of the key implications of Android encryption is the shift in forensic expectations. Traditional assumptions of complete data extraction from seized devices are increasingly impractical. Investigators must now anticipate partial or inaccessible datasets, particularly when devices are encountered in the Before First Unlock (BFU) state. This necessitates cautious interpretation of missing artefacts, as the absence of data does not necessarily indicate the absence of user activity [6].

Encryption also emphasizes the importance of procedural rigor in forensic investigations. Factors such as timing of device seizure, preservation of device state, and accurate documentation of encryption conditions directly influence the volume and quality of recoverable evidence. In practical scenarios, delays in device submission and operational constraints may reduce opportunities for After First Unlock (AFU) analysis, highlighting the need for standardized evidence handling procedures [6].

From a legal standpoint, encryption intensifies the balance between individual privacy and investigative requirements. Courts and legal frameworks increasingly prioritize the integrity, legality, and transparency of digital evidence collection. As encryption restricts access even in lawfully seized devices, forensic practitioners must clearly document examination limitations and justify their methodologies. Transparent reporting of such constraints enhances evidentiary reliability and supports judicial scrutiny [6], [8].

The challenges posed by encrypted Android devices also highlight the growing importance of multi-source evidence correlation. Mobile device analysis must be supplemented with additional sources such as cloud data, network logs, and service provider records. This integrated forensic approach is particularly relevant in digitally interconnected environments, where user activities extend beyond a single device [4], [6].

Finally, encryption should be viewed not as a temporary barrier but as a persistent characteristic of modern mobile ecosystems. Attempts to bypass encryption through non-standard or unsupported methods risk compromising forensic integrity and legal admissibility[6], [8], [9]. Therefore, the focus must shift toward adaptive forensic frameworks, improved investigative strategies, and continued research aimed at enhancing forensic capabilities within encrypted environments [4], [6].

VII. FUTURE DIRECTIONS IN MOBILE FORENSICS FOR ENCRYPTED ANDROID DEVICES

As encryption continues to evolve as a core component of Android security architecture, mobile forensic practices must adapt to function effectively within encrypted environments rather than attempting to bypass them. Future advancements will require a balanced integration of technical innovation, procedural refinement, and policy-level support to address emerging challenges in forensic investigations [6], [4].

One significant direction is the adoption of context-based and artefact correlation techniques. When direct access to encrypted data is restricted, investigators can derive evidentiary value by correlating metadata, system logs, timestamps, and externally available information. Structured correlation approaches can enhance analytical depth while maintaining forensic integrity and methodological reliability [6], [4].

The integration of cloud forensics represents another critical area for advancement. Many Android applications depend on cloud-based storage and synchronization services, which may retain relevant data even when local device storage is encrypted. In digitally evolving environments such as India, where cloud-enabled financial and communication platforms are widely used, the development of standardized procedures for lawful cloud data acquisition and analysis can significantly strengthen investigative outcomes [4], [6][15].

Artificial intelligence and machine learning techniques also offer promising opportunities in mobile forensics. AI-assisted approaches can support pattern recognition, anomaly detection, and relationship mapping within large volumes of partially accessible data[15]. These techniques may improve triage efficiency, prioritize relevant artefacts, and assist in interpreting incomplete datasets. However, their application must remain transparent, explainable, and aligned with legal admissibility standards to ensure reliability in judicial processes [4], [6].

Another important direction is the standardization of forensic procedures for handling encrypted devices. Establishing clear guidelines for device seizure, documentation of Before First Unlock (BFU) and After First Unlock (AFU) states, evidence preservation, and reporting practices can reduce inconsistencies across forensic laboratories. The development of unified procedural frameworks can enhance investigative efficiency and improve confidence in digital evidence evaluation [6].

Finally, sustained collaboration between forensic researchers, law enforcement agencies, policymakers, and technology developers is essential. As encryption technologies continue to advance, coordinated efforts can help align data security objectives with legitimate investigative requirements. Such collaboration will play a critical role in ensuring that mobile forensic practices remain effective, legally compliant, and ethically sound in increasingly secure digital environments [4], [6].

VIII. CONCLUSION

The increasing adoption of advanced encryption mechanisms in modern Android devices has fundamentally reshaped the landscape of mobile forensic investigations. While encryption plays a critical role in safeguarding user privacy and data security, it simultaneously introduces substantial challenges for forensic practitioners, particularly in environments where timely and comprehensive access to digital evidence is essential [4], [6].

This paper presented an analytical examination of the challenges associated with mobile forensics on encrypted Android devices, with specific reference to the context of India. The evolution of Android security mechanisms—including full disk encryption, file-based encryption, secure boot, and hardware-backed key storage—was analyzed to demonstrate their impact on conventional forensic acquisition techniques[13]. The study highlighted how factors such as Before First Unlock (BFU) and After First Unlock (AFU) states, application-level encryption, and limitations of forensic tools significantly restrict data accessibility and complicate investigative processes [2], [6],[14].

In addition to technical constraints, the study emphasized the importance of legal and procedural considerations in mobile forensic investigations. The need to balance investigative requirements with privacy protections reinforces the importance of lawful, transparent, and well-

documented forensic practices. Furthermore, the findings indicate that mobile forensics must move beyond a purely device-centric approach and adopt integrated strategies that incorporate cloud data, network artefacts, and contextual evidence sources [4], [6].

In conclusion, encryption should be regarded not as a temporary barrier but as a defining characteristic of modern mobile ecosystems. Addressing its impact requires the development of adaptive forensic frameworks, standardized methodologies, and continued research efforts rather than reliance on invasive or unsustainable techniques. By acknowledging the constraints imposed by encryption, forensic practitioners and researchers can enhance the effectiveness, reliability, and legal defensibility of mobile forensic investigations in increasingly secure digital environments [4], [6], [8].

IX. REFERENCES

[1]. Hoog, Andrew, and Strzempka, Katie. (2011). iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices. Elsevier. ISBN: 9781597496598.

[2]. Lessard, Stephen, and Kessler, Gary C. (2010). Android Forensics: Simplifying Cell Phone Examinations. Small Scale Digital Device Forensics Journal, Vol. 4, No. 1, pp. 1–12.

[3]. Zareen, M. R., et al. (2020). Mobile Device Forensics: A Review. IEEE Access, Vol. 8, pp. 181650–181662. DOI: 10.1109/ACCESS.2020.3029807.

[4]. van Baar, Richard, van Beek, Hans, and van Eijk, Eric. (2015). Digital Forensics as a Service. Digital Investigation, Vol. 15, pp. 20–38. DOI: 10.1016/j.diin.2015.07.001.

[5]. National Institute of Standards and Technology (NIST). (2022). SP 800-101 Revision 2: Guidelines on Mobile Device Forensics. NIST Special Publication 800-101 Rev.2.

[6]. Android Open Source Project. (2023). Android Security Overview. Google. Available at: https://source.android.com/security.

[7]. European Union Agency for Cybersecurity (ENISA). (2023). ENISA Mobile Threat Landscape 2023. ENISA Report.

[8]. Government of India. (1872). Indian Evidence Act, Section 65B: Admissibility of Electronic Records. Government of India.[9] O. N. Ravi, “Electronic Evidence: A Need to Amend Sec. 65B of the Indian Evidence Act, 1872,” 2022.

[9]. Ayers, Rick, Brothers, Sam, and Jansen, Wayne. (2014). Guidelines on Mobile Device Forensics. NIST Special Publication 800-101 Revision 1.

[10]. Breeuwsma, Marcel, de Jongh, Martien, Klaver, Coert, van der Knijff, Ronald, and Roeloffs, Mark. (2007). Forensic Data Recovery from Flash Memory. Small Scale Digital Device Forensics Journal, Vol. 1, No. 1, pp. 1–17.

[11]. Casey, Eoghan. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd Edition. Academic Press. ISBN: 9780123742680.

[12]. Al Mutawa, Noura, Baggili, Ibrahim, and Marrington, Andrew. (2012). Forensic Analysis of Social Networking Applications on Mobile Devices. Digital Investigation, Vol. 9, pp. S24–S33. DOI: 10.1016/j.diin.2012.05.007.

[13]. Jansen, Wayne, and Ayers, Rick. (2007). Guidelines on Cell Phone Forensics. NIST Special Publication 800-101.

[14]. Baggili, Ibrahim, Mislan, Richard, and Rogers, Marcus. (2007). Mobile Phone Forensics Tool Testing. Digital Investigation, Vol. 4, pp. 12–20.

[15]. Martini, Ben, and Choo, Kim-Kwang Raymond. (2013). Cloud Storage Forensics: OwnCloud as a Case Study. Digital Investigation, Vol. 10, No. 4, pp. 287–299. DOI: 10.1016/j.diin.2013.08.005.

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE AND TECHNOLOGY

AUTHORS

- Pandule A. B.
- More S.J.
- Gore R.P.
- Deshmukh P.A.
- Pawade V.S.
- Joshi D.C. and Thakare V.J.

ABOUT IJEAST

International journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high - quality research paper in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

JOURNAL METRICS

H-INDEX	i10-INDEX	IJEAST CITATIONS	PEER-REVIEWED & OPEN ACCESS
33	154	9,647 (IJEAST CITATIONS)	PUBLISHED MONTHLY

PEER REVIEWED

All submission are rigorously peer reviewed to ensure quality.

AUTHORS ARE OUR PRIORITY

We value our authors and recognize their contribution to the advancement of research and knowledge.

OPEN ACCESS

Free and unrestricted access to research for all.

GLOBAL REACH

Connecting researchers and professionals worldwide.

TIMELY PUBLICATION

We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

editor@ijeast.com
www.ijeast.com
India

2455-2143