RESEARCH ARTICLE OPEN ACCESS

Forensic Data Acquisition from Mobile Devices Locked by EMI/Loan Management Systems

Gaurav C. Wayal[1], Anirudha N. Pabale[2], Vishal. S.Pawade[3], Dr.Vijay. J. Thakare[4]

1(Assistant Director, Department of Cyber Crime & TASI, Directorate of Forensic Science Laboratory, Mumbai ,Government of Maharashtra Email: wayal.gaurav3@gmail.com)

2 (Scientific Assistant (FACT), Department of Cyber Crime & TASI, Directorate of Forensic Science Laboratory, Mumbai Maharashtra Email: anirudhapabale116@gmail.com)

3 (Deputy Director, Directorate of Forensic Science Laboratory, Mumbai, Government of Maharashtra Email: vishal.dfsl@gmail.com)

4 (Director, Directorate of Forensic Science Laboratory, Mumbai, Government of Maharashtra

Abstract:

Today, smartphones are frequently sold through Equated Monthly Installment (EMI) by Financial lending institutions or small loan schemes, especially in developing countries where high upfront costs limits access. To secure repayments these financial lending institutions use custom software-based locks that restrict phone access when a payment default occurs. While these systems(locks) protect lenders, they pose major challenges for digital forensic to investigations, if such devices become crucial evidence in fraud or cybercrime cases.

This research is based on a real criminal case involving a smartphone that was locked due to a pending loan repayment. The device (smartphone), a Vivo V2348, had active EMI-lock protection and file-based encryption. Using Cellebrite UFED Inseyets forensic tools in a live setup, a full data extraction was successfully performed. A complete and decrypted file system dump was obtained(extracted) from the locked phone, without bypassing or tampering with the device's internal software. The extracted data was then thoroughly analyzed using Cellebrite Physical Analyzer, where all critical user information—such as application data, logs, contacts, messages, and media—was found to be intact.

This case study proves that even when a phone is locked by EMI-based restrictions, digital forensic tools, when used correctly and lawfully, can recover essential evidence. It also confirms that original user data can be safely preserved, interpreted, and presented in a legally acceptable manner, maintaining both accuracy and integrity in forensic reporting.

Keywords — **Mobile Forensics, EMI Lock Bypass, Loan Management System, Android Data Extraction, File-Based Encryption, Cellebrite UFED, Vivo Smartphone Forensics, Digital Evidence, Data Acquisition, Locked Device**

I. INDRODUCTION

Smartphones have become an essential part of daily life across many developing countries. People rely on them not just for communication, but also for accessing online education, digital payments, and remote work opportunities. However, due to their high initial cost, many individuals find it difficult to purchase smartphones outright. To bridge this financial gap, retailers in collaboration with Banks, Non-Banking Financial Companies(NBFCs) have introduced purchasing options like Equated Monthly Installments (EMIs) and small-scale loan schemes. These plans allow users to own smartphones immediately while spreading the payment over a period of time.

To ensure the customers repay their installments on time, lending institutions or vendors install loan management systems on the devices. These are commonly referred to as EMI locks. Unlike security systems that come built into Android—such as Factory Reset Protection (FRP) or Mobile Device Management (MDM)—these EMI locks are often custom-developed by third-party vendors [5][6]. Their primary function is to limit the usability of the device when a payment is overdue. Depending on the design, they can display aggressive payment reminders, restrict access to apps, or completely lock down the device, forcing the user to clear their dues. While this locking mechanism serves a financial purpose for lenders, it presents new challenges to forensic investigators. In criminal cases involving cyber fraud, identity theft, or digital abuse, smartphones often hold vital evidence. However, when a device under EMI lock is submitted for forensic analysis, accessing its data becomes more challenging. Since these lock systems are not part of the standard Android framework and often behave unpredictably, they might include features like remote locking or wiping of data upon tampering [7].

Traditional forensic methods, like those described by Lessard and Kessler [1], and later refined by Hoog [2], usually focus on overcoming typical Android protections such as screen passwords, FRP, or system-level encryption. These procedures are well-documented and integrated into most forensic tools. EMI locks, on the other hand,

work at the application level. While they visually block user access, they typically don't encrypt the actual data. Therefore, it's often still possible to retrieve data from such devices using advanced tools and techniques [9].

With Android versions 10 and higher, file-based encryption (FBE) has become a standard. Under this system, after the user unlocks the device once, it remains in a decrypted state—known as "After First Unlock" or AFU mode [8]. This creates a short but important window for forensic experts to acquire the full file system without breaching data integrity. Modern tools like Cellebrite's Inseyets UFED and Physical Analyzer are built to operate in such conditions, even when logical restrictions like EMI locks are active [7].

Despite the increasing number of phones being sold through EMI schemes, and the rising number of locked devices encountered in forensic labs, there is still limited documentation or case-specific research about EMI locks. Most existing work focuses on bypassing factory-level protections [3], understanding MDM-based controls [5], or decrypting Android's native encryption layers [8]. The technical structure and forensic handling of third-party EMI lock systems have not yet been fully explored. As pointed out by Kumar and Singh [9], although these locks appear secure, they often don't use actual encryption—making them susceptible to lawful data extraction using proper forensic tools and workflows.

This case study addresses that gap by analyzing a real crime case involving a Vivo smartphone (model V2348), which was locked through an active EMI system and running Android 14. Using Cellebrite Inseyets in a live forensic setting, a full decrypted file system was extracted successfully. The phone remained in AFU mode during acquisition, allowing the forensic process to retrieve all internal data intact. This research supports previous findings from Android forensic literature [1][2][4][8] and introduces a practical method for forensic investigators to handle phones affected by non-standard loan management locks.

II. Problem Statement

The growing trend of purchasing smartphones through installment plans has led to the widespread use of EMI and loan management applications that can lock a device when payments are not made. These locks restrict user access by blocking the screen, which creates difficulties during mobile forensic investigations.

Unlike standard Android security features, EMI locks are created by third-party companies and work differently on each device. Because their behavior is not clearly documented, common forensic actions such as restarting the phone or attempting a reset may cause data loss or further restrict access to the device.

Although mobile forensic research covers Android security mechanisms, there is very little guidance on how investigators should handle smartphones affected by EMI locks. This lack of clear procedures increases the risk of damaging or losing digital evidence. Therefore, there is a need to study whether data can be safely and legally extracted from EMI-locked smartphones using forensic tools without affecting the original data.

III. Literature Survey

The growth of mobile forensics has mirrored the rapid expansion of smartphone use and security advancements. Initial foundational work by Lessard and Kessler [1] classified data acquisition into logical, physical, and chip-off techniques, stressing the importance of preserving evidence integrity. Expanding on this, Hoog [2] provided a technical breakdown of Android's security features—such as bootloader processes, application sandboxing, and encryption methods—pointing out key challenges posed by full-disk and file-based encryption (FBE), especially on devices running Android 10 and above.

As Android security mechanisms evolved, researchers turned to bypassing protection layers like Factory Reset Protection (FRP). Satheesh Kumar and Balakrishnan [3] evaluated methods to bypass FRP using tools legally and technically like Cellebrite, Magnet AXIOM, and Oxygen Forensics. At the same time, Quick and Choo [4] addressed the issue of logically locked devices, proposing acquisition techniques during the "After First Unlock" (AFU) state—where encryption keys remain active—allowing forensic access to decrypted user data.

Other research explored Mobile Device Management (MDM) systems due to their relevance to forensic acquisition and their structural resemblance to EMI lock apps. Azfar et al. [5] categorized MDM applications based on control mechanisms, while follow-up work [6] analyzed communication-based Android apps that use overlays, background services, and remote

commands—features now seen in many EMI locking systems. However, EMI locks differ significantly in that they are third-party solutions lacking standardized design and are often undocumented, making them harder to manage during forensic investigations. Cellebrite's documentation [7] notes that many such apps restrict access via overlays without encrypting the data, creating a forensic opportunity if the device is in AFU mode.

File-based encryption and access during AFU were further explored by Islam et al. [8], who confirmed that with proper tools, full data extraction is achievable under certain conditions. Similarly, Kumar and Singh [9] analyzed EMI apps and observed that while they impose control over the device, they rarely encrypt stored data, allowing for potential forensic recovery. While existing literature addresses standard Android security and MDM systems, research on EMI lock mechanisms is limited. This study contributes by demonstrating a successful forensic acquisition of a loan-locked smartphone, supporting evidence extraction even under non-standard locking conditions.

IV. Research Objectives

The main objective of this research is to investigate how mobile forensic investigators can successfully extract data from smartphones that are locked using EMI or loan management applications. These financial lock systems, although designed to enforce repayment, introduce significant obstacles during forensic examinations, particularly in cases involving digital fraud, identity misuse, or cybercrime. Since these locks are not part of Android's standard security framework, understanding their technical structure and behavior is essential for lawful evidence acquisition.

A secondary goal of this study is to determine whether certified forensic tools—specifically Cellebrite Inseyets UFED—can extract a complete file system from such devices without altering or deleting original data. The research focuses on devices in the AFU (After First Unlock) state to evaluate whether decrypted user data, such as application content, call logs, messages, and images, can be retrieved and parsed accurately using analysis tools like UFED Physical Analyzer.

Finally, the study seeks to establish a clear and repeatable forensic workflow for handling EMI-locked smartphones. This includes identifying AFU states, preparing safe acquisition environments, and ensuring that forensic protocols—such as maintaining the chain of custody—are followed throughout the process. The outcomes of this research is intended to bridge a gap in current forensic literature by offering real-world procedures and best practices for ethically managing non-standard device locks during investigations.

V. Methodology

1.1. Tools Used

- Cellebrite Inseyets UFED for physical extraction
- UFED Physical Analyzer for parsing acquired dump
- Supporting logs and screenshots for validation

1.2. Test Device

- Brand: Vivo
- Model: V2348
- OS Version: Android 14
- Security Patch: 2024-10-01
- Encryption: File-based, Hot (decrypted) during extraction

1.3. Procedure

1. Device confirmed to be loan locked

During the initial examination of the test device, it was clearly identified that the smartphone was restricted by a loan management application. This was confirmed through a visible lock screen message prompting the user to complete a pending EMI payment. The lock restricted access to core functions such as the home screen, applications, and system settings. A screenshot taken during this stage captured the active payment reminder overlay, providing clear evidence that the financial lock was engaged and functioning as intended.

Fig. 1 Mobile phone with loan locked screen.

2. Connected to UFED Inseyets workstation

The forensic process began with preparing the UFED Inseyets workstation by updating software and selecting the Android operating system for analysis. The test smartphone was verified to be in a locked state, showing an EMI payment reminder on the screen. It was then connected to the UFED workstation using a compatible cable. The system successfully

detected the device and established a secure connection without changing any data. This setup ensured a safe and forensically sound environment for data extraction.

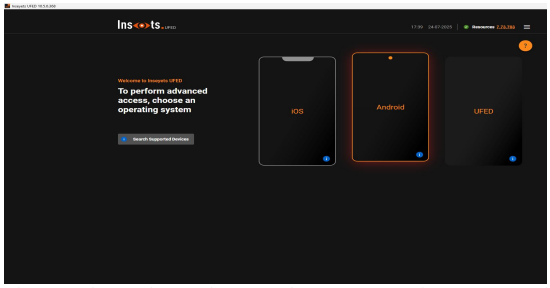

Fig. 2 perform advanced access choses an operating system android

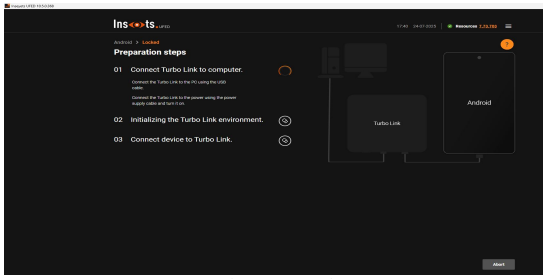

Fig. 3 Preparing steps

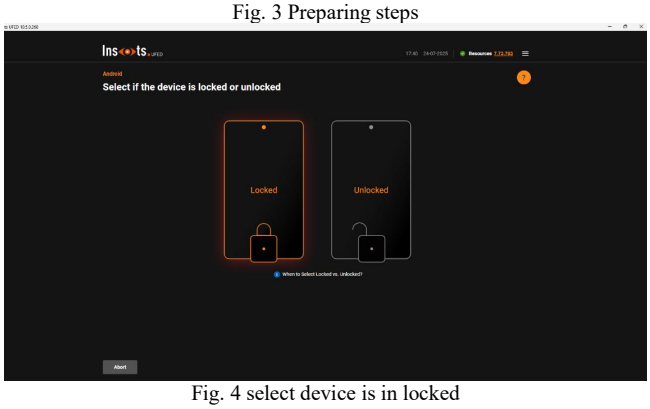

Fig. 4 select device is in locked

3. Device status verified as unlocked for acquisition (AFU: After First Unlock).

After verifying the loan lock, the smartphone was connected to the Cellebrite Inseyets UFED workstation to begin data acquisition. Upon connection, the device's status was assessed and found to be in an AFU (After First Unlock) state. This condition indicated that the device had been successfully unlocked at least once after booting, allowing access to decrypted user data stored in memory—an essential factor for enabling complete and forensically sound data extraction.

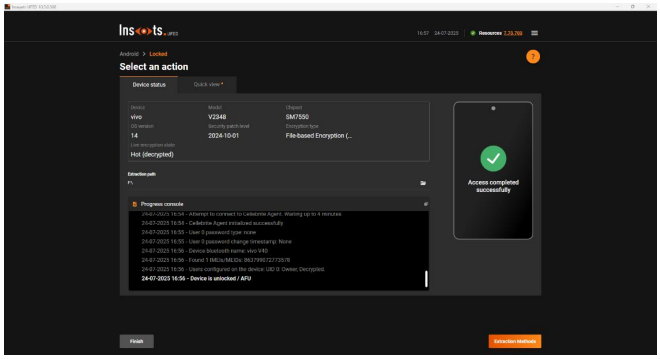

Fig. 5 Mobile Phone Access completed successfully.

4. Full file system extraction initiated and completed

With the device confirmed to be in an accessible AFU state, a full file system extraction was carried out using Cellebrite Inseyets UFED. The process completed successfully, producing a raw data dump totaling approximately 17.92 GB. Throughout the extraction, stable data transfer speeds were maintained, and system-generated logs recorded hash values and integrity checks, confirming that the acquired data remained intact and unaltered.

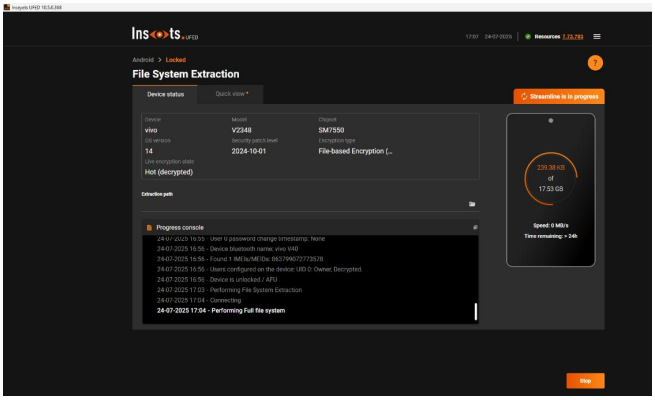

Fig.6 Performing full file system

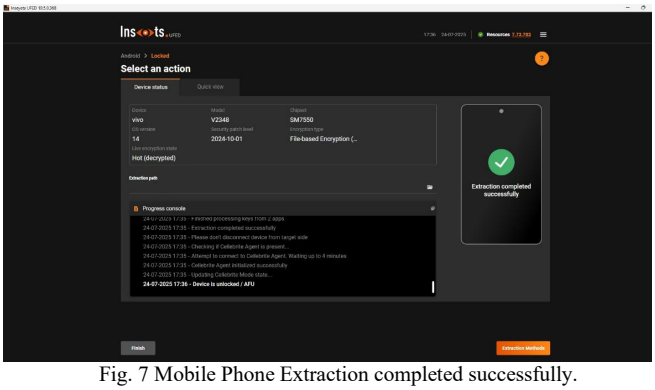

Fig. 7 Mobile Phone Extraction completed successfully.

5. Dump parsed in UFED PA

The extracted data dump was parsed into UFED Physical Analyzer for detailed examination. The analysis confirmed successful recovery of essential user data, including images, messages, call logs, app-related files, and system directories. The presence of decrypted content indicated that the extraction occurred while the device was in an AFU state, allowing access to user data even with the EMI lock interface still active.

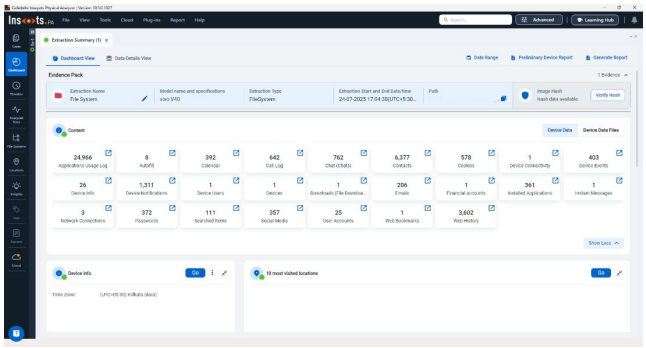

Fig. 8 Extracted data parsed in UFED PA Successfully.

VI. RESULT AND ANALYSIS

The forensic acquisition process yielded a **complete and decrypted file system** extraction from the EMI/loan-locked smartphone. Despite the device being locked at the user interface level, the underlying data storage remained accessible after establishing a trusted connection in AFU (After First Unlock) mode. This reinforces the observation that **loan management locks generally obstruct the graphical interface or user access layer**, but **do not encrypt or restrict access to the device's internal file system** at the hardware or OS level.

The logs recorded during the extraction illustrate several key technical outcomes:

- **Exploitation success**: The device was successfully exploited using *Method 2*, enabling low-level access without requiring screen unlock credentials or physical user interaction.
- **Agent deployment**: Cellebrite Agent was deployed and initialized securely, allowing persistent communication and control over the target phone.
- **Decryption status**: User 0 (device owner) data was marked as **decrypted**, meaning full access to stored content was achieved without password protection.
- **Data scope**: The acquisition recovered extensive user information, including:
  - App data from social media and communication platforms (e.g., Snapchat, WhatsApp, Instagram).
  - Call logs, media files, and other structured data.
- **Data integrity**: File hashes were automatically generated and verified within the UFED Physical Analyzer environment, ensuring that **no data tampering** occurred during the acquisition process.
- **Total extraction size**: Approximately **17.92 GB** of data was extracted and parsed successfully.

The analysis in UFED PA confirmed that all essential forensic artifacts were intact and accessible. This included communications, media, system logs, app encryption keys, and user configuration files. These results demonstrate that **forensic tools can bypass EMI locks**, and that **data from EMI-locked devices can be reliably acquired for investigation**, provided the device has been unlocked once (AFU) and is vulnerable to supported extraction methods.

VII. DISCUSSION

This study confirms that with proper authorization and advanced forensic tools, data can be successfully acquired from smartphones locked by EMI or loan apps. These locks mainly block user access at the interface level but do not encrypt the underlying file system. The use of live acquisition in the AFU (After First Unlock) state proved effective, especially on Android devices with file-based encryption.

By leveraging Cellebrite UFED, decrypted user data such as app credentials, media, and full system files were recovered without damaging evidence. As EMI-locked phones become more common in digital lending, this method offers a reliable approach for forensic investigators to extract data safely and lawfully in real-world cases.

VIII. CONCLUSION

This study confirms that full file system extraction from EMI-locked smartphones is both technically achievable and forensically sound when using tools like Cellebrite UFED. Despite interface-level restrictions by loan management apps, user data—including decrypted files and application content—can be accessed without altering or damaging evidence. These findings address a major forensic challenge and provide a validated method for lawful data recovery from financially locked Android devices.

IX. FUTURE WORK

1. **Test on Different Loan Lock Vendors**
   Future studies should examine a broader range of EMI/loan management apps across multiple brands and regions to understand how each implements device restrictions.
2. **Analyze More Device Models and OS Versions**
   Expanding tests to include various Android

versions and smartphone models will help determine the consistency and reliability of extraction methods across platforms.

3. **Compare Other Forensic Tools**
   Comparing Cellebrite with tools like Oxygen Forensics or Magnet AXIOM could provide insights on tool-specific strengths and limitations in handling locked devices.

REFERENCES

1. *Lessard, J., & Kessler, G. (2010). Android Forensics: Simplifying Cell Phone Examinations. Small Scale Digital Device Forensics Journal.*
2. *Hoog, A. (2011). Android Forensics: Investigation, Analysis, and Mobile Security for Google Android. Elsevier.*
3. *Satheesh Kumar, V., & Balakrishnan, V. (2019). A Review of Bypass Techniques for Android FRP Lock. IJEAT.*
4. *Quick, D., & Choo, K. K. R. (2014). Google Android Forensics: A Review of Forensic Features. Digital Investigation.*
5. *Azfar, A., Choo, K. K. R., & Liu, L. (2015). Forensic Taxonomy of Popular Android MDM Applications. Journal of Digital Forensics, Security and Law.*
6. *Azfar, A., Choo, K. K. R., & Liu, L. (2017). An Android Communication App Forensic Taxonomy. Future Generation Computer Systems.*
7. *Cellebrite. (2023). UFED Inseyets User Guide. Cellebrite Technical White Paper.*
8. *Islam, R., et al. (2022). Decrypting Android 10+ File-Based Encryption for Forensics: A Practical Analysis. Digital Investigation.*
9. *Kumar, P., & Singh, V. (2021). Loan Management Apps and Mobile Privacy: A Security Analysis. Journal of Mobile Security.*
10. *Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Elsevier.*