Mobile Forensic Analysis and Data Extraction for Android Devices

A Multi-Tool Approach for Efficient Digital Evidence Extraction and Analysis

[1] Badam Navya Sri Bala, [2] Routhu Keerthy, [3] Gangapuram Rohith, [4] Dr. Shraban Kumar Apat
[1,2,3] Bachelor of Technology Student, [4] Associate Professor
[1,2,3,4] CSE – Cyber Security
[1,2,3,4] Geethanjali College of Engineering and Technology (GCET), Hyderabad, India
[1]badamnavyasribala@gmail.com, [2]routhukeerthy@gmail.com, [3]gangapuramrohith123@gmail.com, [4]shraban.cse@gcet.edu.in

***Abstract*—Mobile devices have turn out to be a number one source of virtual evidence in contemporary cybercrime investigations, in particular due to the widespread use of Android smartphones. Extracting and analyzing data from those devices is tough because of encryption mechanisms, confined report systems, and complex utility architectures. This paper gives a complete mobile forensic framework for Android gadgets that integrates more than one tools to make sure green and reliable proof collection. The proposed technique makes use of Android Debug Bridge for logical information extraction, Magnet AXIOM for forensic imaging and deep evaluation, and Mobile Security Framework for utility-level investigation. The machine allows the retrieval of crucial artifacts including call logs, SMS, contacts, media files, and application facts while preserving forensic integrity. The consequences demonstrate that a multi-device methodology substantially improves the accuracy, completeness, and performance of virtual investigations as compared to traditional single-device approaches. This work gives a realistic and scalable answer for cybersecurity experts and law enforcement organizations involved in cell forensic analysis.**

***Index Terms*—Mobile Forensics, Android, ADB, Magnet AXIOM, MobSF, Digital Evidence, Forensic Integrity.**

I. Introduction

The rapid development of telephone generation has drastically expanded the extent of virtual facts generated and stored on cell phones. Android smartphones, being the most extensively used devices, have end up crucial assets of virtual evidence in cybercrime investigations. Mobile forensics performs a vital position in identifying, accumulating, preserving, and analyzing these statistics in a legally admissible manner.

However, current Android systems gift several demanding situations due to encryption mechanisms, restricted get right of entry to machine directories, and complicated utility architectures. Data is frequently disbursed across a couple of layers, inclusive of system storage, utility databases, and cloud services, making extraction and analysis a complicated method.

To cope with these demanding situations, this paper proposes a comprehensive forensic workflow that integrates more than one tools, along with Android Debug Bridge (ADB), Magnet AXIOM, and Mobile Security Framework (MobSF). This multi-tool approach ensures efficient statistics acquisition, deep evaluation, and renovation of proof integrity. The device is designed to provide correct and dependable forensic effects appropriate for real-world cybersecurity investigations.

II. Literature Review

Mobile forensic analysis has advanced drastically over the years, with researchers featuring numerous strategies and tools to enhance the efficiency and accuracy of investigations.

Kumar, Rashid, and Narayan (2025) performed a comparative examine of cell forensic tools for Android devices. Their studies evaluated equipment consisting of ADB, Autopsy, Belkasoft, and Magnet AXIOM, focusing on their capacity to extract extraordinary varieties of forensic artifacts. The examine concluded that Magnet AXIOM and Autopsy offer the maximum comprehensive records extraction skills, although some gear may exchange accuracy for velocity. This locating supports the usage of Magnet AXIOM on this project for deep forensic analysis. [4]

Patel and Mann (2025) supplied an in-depth survey on mobile digital forensics, highlighting the taxonomy, equipment, and challenges within the area. Their observe emphasised that no single forensic device is enough to address all forms of facts extraction and evaluation. They diagnosed main challenges which include encryption, proprietary records codecs, and cloud integration. This reinforces the need for a multi-device method, which is applied within the proposed machine using ADB, Magnet AXIOM, and MobSF.[5]

Lin et al. (2018) brought an automated forensic evaluation technique for Android packages using static evaluation strategies. Their device, called Fordroid, makes use of taint evaluation to discover touchy records and reconstruct application databases. The have a look at demonstrated that automated static evaluation can effectively locate hidden data and alertness conduct. This concept is immediately carried out in this task thru the usage of MobSF for analyzing APK documents and figuring out vulnerabilities. [6]

Skulkin, Tindall, and Tamma (2018) provide a comprehensive observe on Android forensics, that specialize in contemporary equipment and techniques used for the acquisition and analysis of digital evidence from Android gadgets. Their paintings emphasize the importance of understanding the Android operating machine structure, report systems, and application information systems to carry out effective forensic investigations. The authors discuss various techniques of records extraction, along with logical, bodily, and file device acquisition, and highlight the role of tools along with ADB and superior forensic platforms in retrieving artifacts like name logs, messages, and application statistics. They additionally address challenges which include information encryption, tool safety mechanisms, and anti-forensic techniques. This examine is enormously applicable to the proposed gadget as it helps the use of a multi-device technique and structured workflow for efficient and reliable mobile forensic analysis. [3]

Additionally, Aziz, Mokhti, and Nozri (2015) proposed a established method for cell tool forensic cs along with four key tiers: renovation, facts collection, analysis, and reporting. Their paintings emphasized the importance of keeping proof integrity and following a scientific technique. The technique used in this mission aligns with this framework, making sure that each one forensic process are performed in a legally sound manner.[7]

Overall, the literature certainly shows that a based, multi-device method is vital for effective cellular forensic investigations. The proposed machine builds upon these research contributions to provide a comprehensive and reliable forensic solution.

III. System Design and Methodology

Limitations of Existing System

Existing cellular forensic structures face several obstacles:

- Dependence on unmarried equipment effects in incomplete statistics extraction
- Difficulty in getting access to encrypted and guarded directories
- Lack of integration among one of a kind forensic tool
- Manual analysis increases effort and time
- Limited functionality to investigate third-celebration applications
- Higher possibility of missing essential proof

System Architecture

The proposed device follows a layered architecture designed to ensure green facts acquisition and analysis. The structure consists of the following components:

The goal Android device acts because the number one supply of virtual evidence. It is attached to a forensic laptop, which serves as the valuable surroundings for executing forensic equipment. The information acquisition layer is accountable for extracting information using ADB and Magnet AXIOM. The analysis engine strategies the extracted records and plays application analysis the usage of MobSF. Finally, the reporting module compiles all findings right into a established forensic record.

This architecture ensures that each degree of the forensic method is certainly defined and that records integrity is maintained in the course of the research.

Proposed System

The proposed gadget integrates a couple of forensic gear into a unified workflow. Unlike traditional methods, which rely upon a single device, this device combines logical extraction, forensic imaging, and alertness evaluation.

The device is capable of extracting a wide range of virtual proof, inclusive of communique information, utility records, and gadget documents. It also plays vulnerability evaluation of applications, offering deeper insights into capacity protection threats.

By combining distinct tools, the gadget overcomes the constraints of character gear and affords a extra comprehensive forensic analysis.

Methodology

The technique follows a structured workflow aligned with popular virtual forensic procedures, making sure systematic acquisition, evaluation, and reporting of virtual proof while preserving its integrity.

The process begins with making ready the Android tool with the aid of allowing USB debugging and organising a stable reference to the forensic workstation. This step ensures controlled verbal exchange among the tool and forensic tools.

Once the relationship is mounted, logical records extraction is accomplished using Android Debug Bridge (ADB). Various instructions are done to retrieve critical artifacts such as call logs, SMS messages, contacts, and media files. This step gives short get entry to to important person information required for initial analysis.

Next, software-particular facts is extracted from the tool garage. This includes retrieving databases and files related to packages which includes WhatsApp and Instagram. These data sources contain precious forensic information which includes chat records, media content material, and consumer interactions.

The manner then proceeds to forensic imaging using Magnet AXIOM. A forensic photograph of the tool is created to permit in-intensity analysis and restoration of hidden or inaccessible facts. This step guarantees that a complete reproduction of the tool records is to be had for exam without changing the original proof.

Finally, application analysis is done the use of the Mobile Security Framework (MobSF). APK files are analyzed to become aware of permissions, vulnerabilities, and capability security risks. This helps in information utility conduct and detecting malicious sports.

The outputs obtained from all equipment are then correlated and compiled right into a comprehensive forensic file, presenting a whole view of the extracted evidence.

IV. RESULTS AND DISCUSSIONS

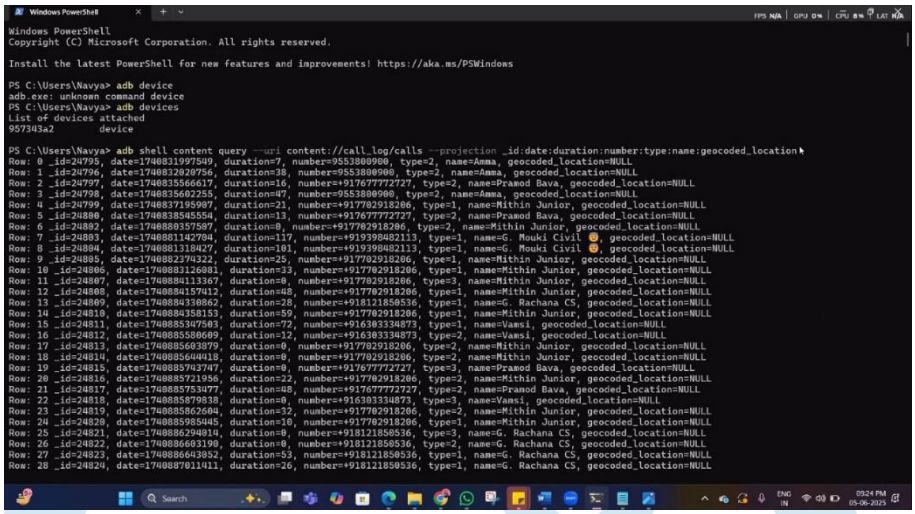

Fig 1 ADB Call Log Extraction

The output represents the extraction of name log records the use of ADB instructions. The retrieved records include telephone numbers, timestamps, and make contact with periods. This fact is crucial for reconstructing communique styles and figuring out interactions among people throughout forensic investigations.

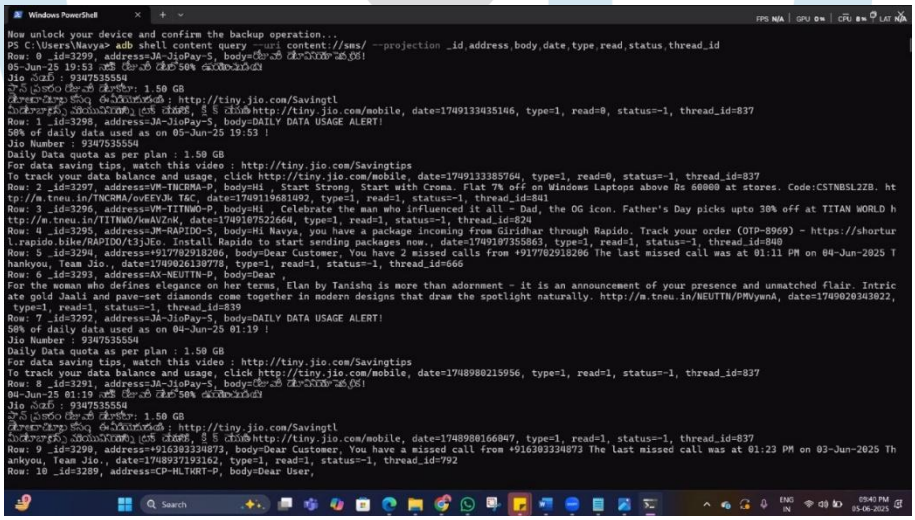

Fig 2 ADB SMS Data Extraction

The extracted SMS records include message content in conjunction with sender and receiver info. The presence of timestamps allows investigators to establish a series of verbal exchange events, which is important in reading consumer conduct and interactions.

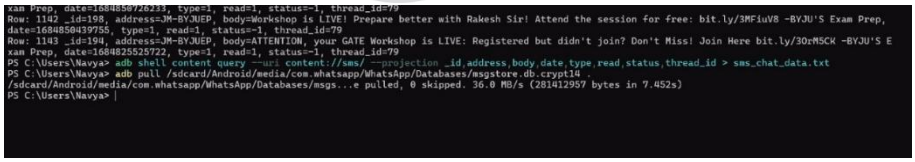

Fig 3 WhatsApp Database Extraction

The extracted WhatsApp database report includes saved chat records, media references, and user interaction statistics. This statistic affords deeper insights into user communique and performs a important role in forensic investigations related to messaging packages.

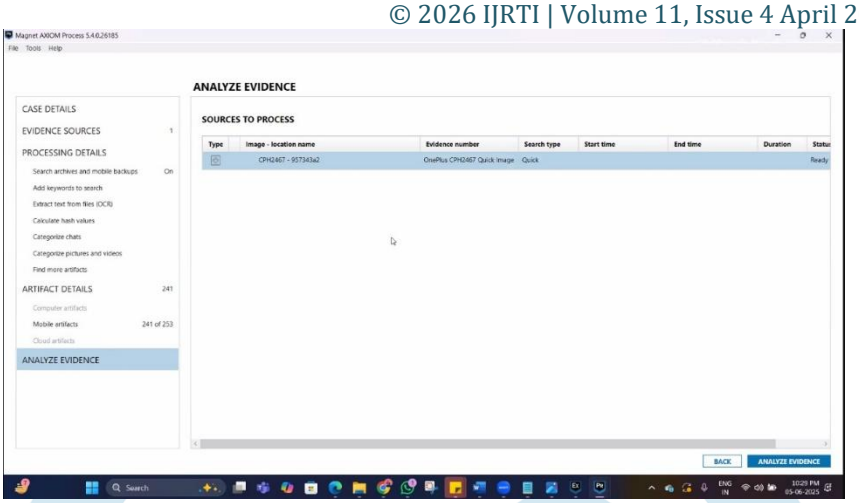

Fig 4 Magnet AXIOM Device Detection

The system identifies the linked Android device as a valid evidence supply within the Magnet AXIOM environment.

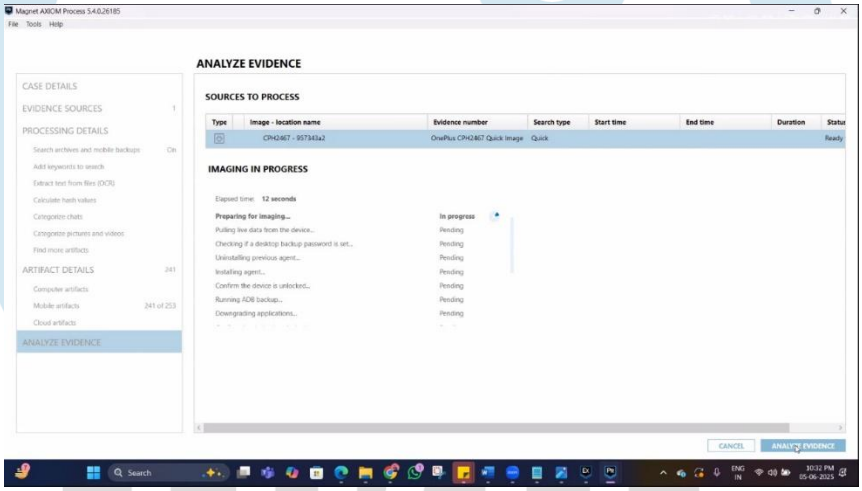

Fig 5 Magnet AXIOM Data Acquisition Process

This phase represents the configuration and initiation of the forensic acquisition system. The device prepares to seize tool records, along with stay facts and file device artifacts. This step ensures that a comprehensive picture of the tool is created for particular analysis.

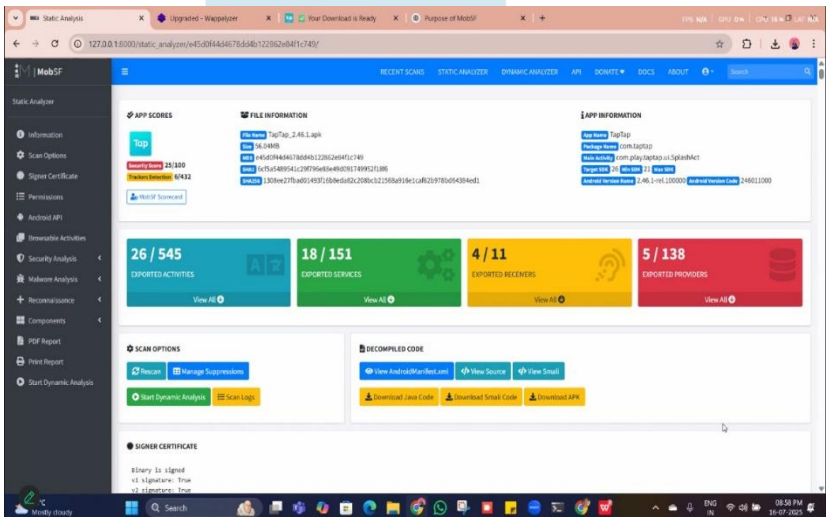

Fig 6 MobSF Application Analysis

The output provides the outcomes of static evaluation achieved on an Android software. It consists of details about application permissions, API utilization, and capacity vulnerabilities. This fact enables in figuring out security dangers and understanding how applications take care of touchy facts.

V. Conclusion

This paper provides a complete and structured method for cell forensic evaluation and data extraction from Android devices. The proposed system integrates more than one forensic equipment, namely Android Debug Bridge (ADB), Magnet AXIOM, and Mobile Security Framework (MobSF), to triumph over the restrictions of traditional unmarried-device strategies. The methodology ensures systematic acquisition, analysis, and reporting of digital evidence whilst retaining forensic integrity.

The implementation consequences show that ADB is effective for short and focused extraction of user-degree information which includes call logs, SMS messages, and alertness documents. Magnet AXIOM enhances the investigation by permitting deep forensic imaging and recovery of hidden or inaccessible facts. MobSF further strengthens the evaluation with the aid of supplying insights into software conduct, permissions, and capacity security vulnerabilities.

The mixture of those equipment consequences in a unified and green forensic workflow capable of extracting various varieties of virtual evidence. The method improves accuracy, reliability, and completeness of investigations, making it appropriate for actual-world programs in cybersecurity and virtual forensics. Overall, the proposed gadget provides a realistic and scalable answer for studying Android gadgets in forensic investigations.

VI. Future Scope

The proposed device may be further better by way of extending its abilties and incorporating superior technology. Future enhancements may additionally encompass:

- Support for forensic analysis of iOS and different mobile working structures
- Integration of cloud forensics to research records stored in on line structures
- Automation of forensic workflows the use of artificial intelligence and machine getting to know strategies
- Development of real-time records acquisition and monitoring structures
- Enhancement of user interfaces to provide better visualization and reporting of forensic findings
- Implementation of advanced techniques for managing encrypted and guarded data

These improvements will in addition enhance the efficiency, scalability, and applicability of cellular forensic structures, enabling investigators to address greater complex and evolving cybercrime situations.

REFERENCES

[1] Hoog, Andrew. Android forensics: investigation, analysis and mobile security for Google Android. Elsevier, 2011.

[2] Bommisetty, Satish, Rohit Tamma, and Heather Mahalik. Practical mobile forensics. Packt Publishing, 2014.

[3] Skulkin, Oleg, Donnie Tindall, and Rohit Tamma. Learning Android Forensics: Analyze Android devices with the latest forensic tools and techniques. Packt Publishing Ltd, 2018.

[4] Kumar, Prince, Ekbal Rashid, and Ritushree Narayan. "A Comparative Study of Mobile Forensic Tools for Android Devices." Recent Advances in Artificial Intelligence for Sustainable Development (RAISD 2025). Atlantis Press, 2025.

[5] Patel, Bhavini, and Palvinder Singh Mann. "A Survey on Mobile Digital Forensic: Taxonomy, Tools, and Challenges." Security and Privacy 8.2 (2025): e470.

[6] Lin, Xiaodong, et al. "Automated forensic analysis of mobile applications on Android devices." Digital Investigation 26 (2018): S59-S66.

[7] Aziz, Normaziah A., Fakhrulrazi Mokhti, and M. Nadhar M. Nozri. "Mobile device forensics: extracting and analysing data from an android-based smartphone." 2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec). IEEE, 2015.