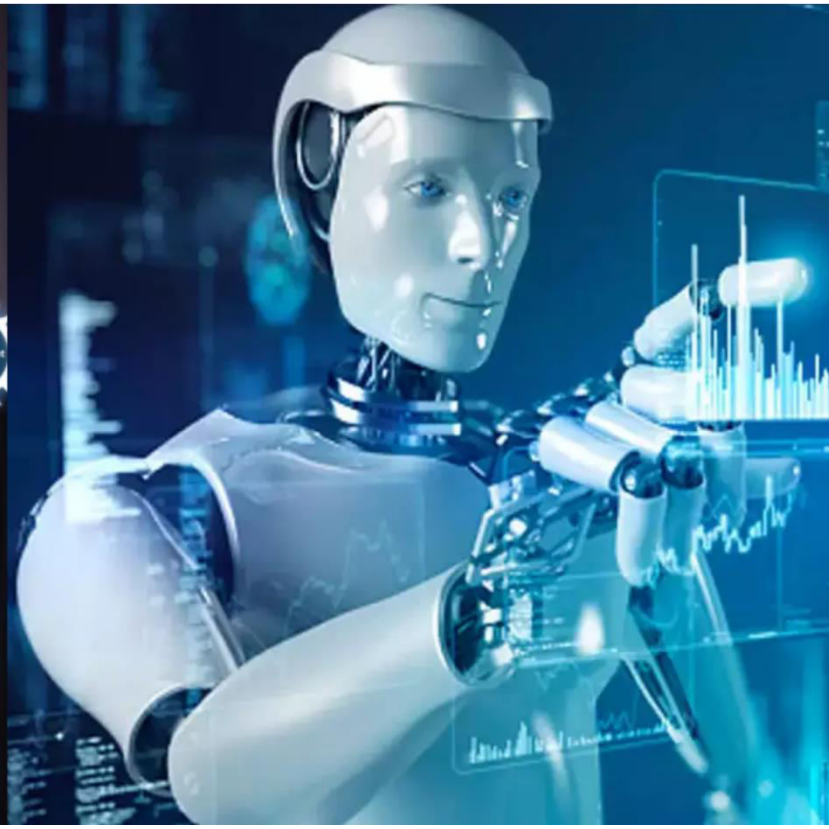
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*

**Impact Factor: 8.699**

**Volume 15, Issue 2, February 2026**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502072|

# Mobile Forensic Toolkit for Android Devices (Using ADB)

**Aparna S[1], Delshiny D[1], Jeena Femi I A[1], Jonisha S[2]**

Department of Information Technology, Arunachala College of Engineering for Women, Manavilai, Vellichanthai, Tamil Nadu, India[1]

Assistant Professor, Department of Information Technology, Arunachala College of Engineering for Women, Manavilai, Vellichanthai, Tamil Nadu, India[2]

**ABSTRACT:** The rapid proliferation of Android smartphones has made mobile devices a crucial source of digital evidence in modern criminal and cybercrime investigations. However, the diversity of Android platforms, strong security mechanisms, and dependence on expensive proprietary forensic tools pose significant challenges for effective and forensically sound data acquisition. This paper presents the design and implementation of a Mobile Forensic Toolkit for Android Devices using Android Debug Bridge (ADB), aimed at providing a cost-effective, automated, and reliable solution for logical data acquisition without requiring device rooting. The proposed toolkit enables secure device detection, logical extraction of critical forensic artifacts such as contacts, call logs, SMS/MMS messages, and multimedia files, and ensures evidence integrity through cryptographic hashing using MD5 and SHA-256 algorithms. Extracted raw data from SQLite, XML, and JSON sources is automatically parsed into structured, human-readable formats, facilitating efficient analysis. Additionally, the toolkit generates comprehensive forensic reports in both PDF and HTML formats, including device metadata, timestamps, and hash values, making them suitable for legal and investigative use. Experimental evaluation conducted on multiple Android devices across different OS versions demonstrates high accuracy in data extraction, consistent integrity verification, and reliable report generation. While access limitations exist for non-rooted devices, the toolkit successfully maintains forensic soundness and repeatability. The results indicate that the proposed ADB-based forensic toolkit offers a practical and legally defensible approach for Android mobile forensics, making it valuable for law enforcement agencies, forensic investigators, and academic research. Furthermore, the modular architecture of the toolkit allows easy extensibility to support additional Android artifacts and future OS versions. This work contributes toward strengthening accessible and open forensic solutions by bridging the gap between practical investigative needs and forensic reliability standards.

**KEYWORDS:** Mobile Forensics, Android Forensics, Android Debug Bridge (ADB), Digital Evidence, Logical Data Acquisition, Evidence Integrity, Cryptographic Hashing, Forensic Reporting, SQLite Data Parsing, Cybercrime Investigation.

## I. INTRODUCTION

The widespread adoption of smartphones has transformed the way individuals communicate, store information, and conduct daily activities. Among mobile operating systems, Android dominates the global market due to its open architecture, device diversity, and extensive application ecosystem. As a result, Android smartphones have become a significant source of digital evidence in criminal investigations, cybercrime incidents, and civil litigation. Call logs, short message service (SMS) records, multimedia files, application data, and system logs stored on mobile devices often provide crucial insights into user behaviour, timelines, and intent.

Mobile forensics is a specialized branch of digital forensics that focuses on the identification, acquisition, preservation, analysis, and presentation of evidence from mobile devices in a forensically sound manner. However, Android forensics presents unique challenges due to frequent operating system updates, hardware fragmentation, strong encryption mechanisms, and manufacturer-imposed security restrictions. These challenges often limit investigators' ability to access critical data, particularly on non-rooted devices, without compromising evidence integrity.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502072|

Commercial mobile forensic tools offer comprehensive solutions but are often costly, proprietary, and inaccessible to smaller forensic laboratories, academic institutions, and independent investigators. In contrast, open-source and command-line tools such as the Android Debug Bridge (ADB) provide a standardized and widely supported interface for interacting with Android devices. ADB enables logical data acquisition without requiring device rooting, thereby reducing the risk of data modification and preserving forensic integrity. Despite its capabilities, ADB is primarily command-driven and requires technical expertise, making manual forensic acquisition time-consuming and error-prone.

To address these limitations, this paper presents the development of a Mobile Forensic Toolkit for Android Devices using ADB that automates the processes of device detection, logical data acquisition, integrity verification, data parsing, and report generation. The proposed toolkit integrates cryptographic hashing mechanisms to ensure evidence authenticity and produces structured forensic reports suitable for legal proceedings. By emphasizing accessibility, automation, and forensic soundness, this work aims to provide a practical and cost-effective solution for Android mobile forensics applicable to law enforcement, forensic practitioners, and academic research.

## II. LITERATURE REVIEW

Mobile forensics has emerged as a critical domain within digital forensics due to the increasing reliance on smartphones for communication, data storage, and online services. Android devices, in particular, present unique forensic challenges because of their open architecture, frequent operating system updates, diverse hardware platforms, and enhanced security mechanisms such as encryption and sandboxing.

Early studies in mobile forensics primarily focused on logical data acquisition techniques. Lessard and Kessler (2010) explored the feasibility of extracting user-level data such as contacts, call logs, and SMS messages from Android devices using logical acquisition methods. Their work highlighted that while logical extraction is non-invasive and preserves device integrity, it is limited to data accessible through the operating system and cannot recover deleted or encrypted artifacts.

Several researchers have examined the role of Android Debug Bridge (ADB) in forensic investigations. Distefano et al. (2010) demonstrated that ADB commands could be effectively used to extract application data and system files without rooting the device. This approach was found to be forensically sound when used in a read-only manner. Similarly, Vidas et al. (2011) analyzed the forensic implications of ADB usage and emphasized the importance of hash verification to prevent unintentional data modification during acquisition.

Commercial forensic tools such as Cellebrite UFED, Oxygen Forensic Suite, and XRY have been widely studied for their comprehensive extraction and analysis capabilities. Research by Quick and Choo (2014) compared these tools and reported high accuracy in data extraction across multiple Android versions. However, these tools are expensive, proprietary, and often require licensing, which limits their accessibility for academic institutions and small forensic laboratories. Additionally, compatibility issues may arise with newer Android versions or specific device manufacturers. Open-source forensic tools and frameworks have been proposed as alternatives to commercial solutions. Tools such as Autopsy, Andriller, and AFLogical provide logical acquisition and limited parsing capabilities. Anglano (2014) focused on forensic analysis of WhatsApp data using ADB-based acquisition methods, demonstrating that valuable application-level evidence can be retrieved without rooting. However, these tools often lack integrated reporting mechanisms and require significant manual effort for data interpretation.

Evidence preservation and integrity verification have been emphasized as fundamental requirements in forensic investigations. Casey (2011) highlighted the importance of cryptographic hashing techniques such as MD5 and SHA-256 to ensure the authenticity and admissibility of digital evidence. Studies consistently stress that maintaining a clear chain of custody and repeatable acquisition procedures is essential for legal acceptance.

Recent research has explored automation and intelligence-driven forensic systems. Kumar et al. (2018) proposed an automated ADB-based framework that reduced manual intervention in data extraction and improved efficiency. More advanced approaches integrate machine learning techniques to detect anomalies, malware, or suspicious activity within extracted datasets. Despite these advancements, many solutions remain complex, resource-intensive, or inaccessible to non-specialist users.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502072|

From the reviewed literature, it is evident that while ADB-based logical acquisition is a reliable and non-intrusive approach for Android forensics, there is a lack of lightweight, fully automated toolkits that combine acquisition, integrity verification, parsing, and standardized reporting. This research addresses these gaps by proposing a cost-effective, automated Mobile Forensic Toolkit using ADB that emphasizes forensic soundness, usability, and legal compliance.

## III. METHODOLOGY

This study adopts a descriptive and experimental research methodology to design, develop, and evaluate a Mobile Forensic Toolkit for Android devices using Android Debug Bridge (ADB). The methodology focuses on achieving forensically sound logical data acquisition, integrity preservation, automated parsing, and standardized reporting without requiring device rooting. The research involves the systematic development of modular components that automate device detection, evidence extraction, cryptographic hash generation, and report creation. Experimental evaluation is carried out on multiple Android devices running different operating system versions to assess extraction accuracy, integrity consistency, and repeatability of results. The effectiveness of the toolkit is measured based on successful data acquisition, verification of hash values, and completeness of generated forensic reports, ensuring the proposed system meets practical investigative and legal requirements.

- **System Architecture Overview**

The proposed toolkit follows a modular architecture consisting of five primary components: device connection and detection, data acquisition, evidence preservation, data parsing, and report generation. Each module operates independently to ensure scalability, maintainability, and forensic reliability. Communication between the forensic workstation and the Android device is established using ADB over a secure USB connection.

- **Device Connection and Authorization**

Android devices are connected to the forensic workstation via USB with USB debugging enabled. The toolkit uses ADB commands to detect authorized devices and retrieve device metadata such as model number, Android version, and serial number. This step ensures proper device identification and prevents unauthorized access before data acquisition begins.

- **Logical Data Acquisition**

Logical data acquisition is performed using standard ADB pull commands to extract user-accessible forensic artifacts without modifying the device contents. The extracted artifacts include contacts, call logs, SMS/MMS messages, and multimedia files. System and application databases stored in SQLite format are copied from accessible directories, while media files are retrieved from external storage paths. This approach minimizes the risk of data alteration and maintains forensic soundness.

- **Evidence Preservation and Integrity Verification**

To ensure the authenticity and integrity of the extracted evidence, cryptographic hash values are generated for each acquired file using MD5 and SHA-256 algorithms. Hash values are recorded immediately after extraction and verified throughout the analysis process. This mechanism provides a reliable method for detecting any unauthorized modifications and supports the legal admissibility of the evidence.

- **Data Parsing and Structuring**

Raw forensic data obtained from SQLite, XML, and JSON sources is automatically parsed using Python scripts. The parsed data is converted into structured and human-readable formats such as JSON and CSV, enabling efficient analysis and interpretation by investigators. This step improves readability while preserving the original data semantics.

- **Report Generation**

The toolkit generates comprehensive forensic reports in both PDF and HTML formats. Reports include device information, extracted artifacts, cryptographic hash values, timestamps, and acquisition logs. The standardized reporting format ensures clarity, traceability, and suitability for legal and investigative purposes.

- **Experimental Setup and Evaluation**

The proposed toolkit was evaluated on multiple Android devices running different operating system versions. Performance metrics such as data extraction accuracy, hash consistency, parsing reliability, and report completeness were assessed. The evaluation confirms the effectiveness, repeatability, and forensic reliability of the toolkit under various conditions.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502072|

- **Research Design and Methodology**

This study adopts a descriptive and experimental research design aimed at developing and evaluating a Mobile Forensic Toolkit for Android devices using Android Debug Bridge (ADB). The methodology emphasizes forensically sound logical data acquisition without requiring device rooting, ensuring the integrity and authenticity of extracted digital evidence. Systematic steps are followed, including device detection, automated data extraction, cryptographic hash generation for evidence preservation, data parsing into structured formats, and standardized report generation.

## IV. ARCHITECTURE

The architecture depicts a structured workflow for a mobile forensic toolkit, starting with a forensic workstation, which serves as the central system for managing the forensic process. The workstation establishes a connection with the mobile device through a forensic connection and detection layer, utilizing an ADB interface and device authentication to securely access the device without compromising its integrity.

Once the connection is established, data acquisition occurs, involving the extraction of call logs, messages, contacts, and media files from the device to ensure all relevant digital evidence is captured. Following the acquisition, evidence preservation mechanisms are applied, including hashing techniques such as MD5 and SHA-256 to verify data integrity and ensure that the information remains unaltered during the forensic process.

After preservation, the extracted data undergoes parsing and analysis, with structured processing of formats like SQLite, XML, and JSON, organizing the data for easier interpretation. The processed data is then used for report generation, creating both PDF and HTML reports to document the findings systematically. Finally, these reports and logs serve legal and investigative purposes, while also forming an evidence archive that maintains a comprehensive record of the data collected and the analytical processes applied. This architecture ensures a controlled, verifiable, and methodical approach to mobile device forensics.

In addition to the structured workflow, the mobile forensic toolkit architecture emphasizes security and compliance at every stage. The use of device authentication ensures that the forensic process does not inadvertently alter or damage the data on the mobile device, which is critical for maintaining admissibility in legal proceedings. Furthermore, the toolkit often includes mechanisms for handling both live data acquisition and logical or physical imaging, allowing forensic investigators to tailor their approach based on the type of device and the nature of the investigation. By integrating hashing and integrity verification at the preservation stage, the architecture provides a robust mechanism to demonstrate that the extracted evidence is both authentic and untampered, which is essential for establishing credibility in courts or during regulatory reviews. Maintaining a centralized evidence archive enables efficient long-term case management, allowing prior investigations to be retrieved for comparison or follow-up while ensuring the forensic process remains auditable, repeatable, and defensible.

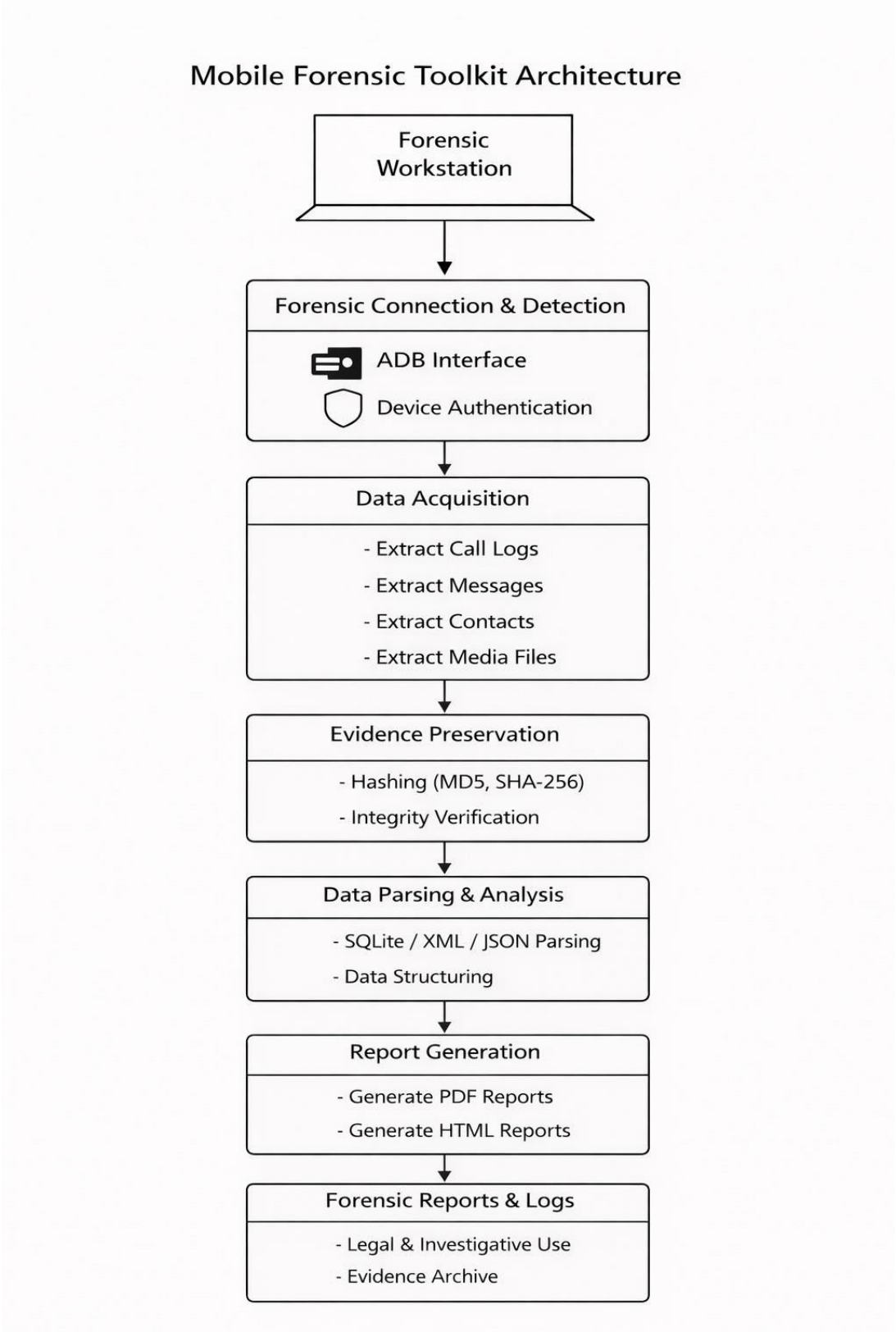
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502072|



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502072|

**Implementation**

The Mobile Forensic Toolkit was implemented using a layered architecture, which separated key functionalities into independent modules to ensure reliability, scalability, and maintainability. The toolkit was developed primarily with Python for scripting ADB commands, handling data extraction, and parsing databases. PDF and HTML report generation was incorporated for forensic reporting.

**Modules Implemented:**

**Device Layer:** Android devices with USB Debugging enabled.
**Communication Layer:** ADB interface to detect and interact with devices.
**Extraction Layer:** Pulls contacts, call logs, SMS/MMS, and media files.
**Evidence Preservation Layer:** Generates MD5 and SHA-256 hashes for extracted data to ensure integrity.
**Parsing Layer:** Converts SQLite, XML, and JSON files into readable formats (JSON/CSV).
**Reporting Layer:** Generates structured PDF and HTML reports for legal and investigative purposes.
**Storage Layer:** Securely stores extracted data and logs for future reference.
**Implementation Environment:**
**Platform:** Windows 10 with Android SDK installed.
**Test Devices:** Samsung Galaxy A50 (Android 11), Google Pixel 4a (Android 12).
**Tools/Libraries:** Python 3.x, SQLite browser, ReportLab/pdfkit, Hashlib.

**Implementation Workflow:**

- Device detection using adb devices to ensure only authorized devices are processed.
- Logical data acquisition via adb pull, supporting both rooted and non-rooted devices.
- Integrity verification using MD5 and SHA-256 hashes for all extracted files.
- Parsing raw databases and media metadata into structured, human-readable formats.
- Generating PDF and HTML reports containing extracted data, timestamps, and hash values.
- Secure storage of evidence and logs for compliance and audit purposes.

**Key Features Achieved:**

- Reliable device detection and communication.
- Successful extraction of forensic artifacts from both rooted and non-rooted devices.
- Maintained forensic integrity through cryptographic hash verification.
- Efficient parsing of raw data into structured formats.
- Comprehensive reporting suitable for investigative or legal review.
- Modular design for ease of maintenance, updates, and potential future enhancements.
- The modular separation of functions allowed each component to operate independently, improving performance, reducing errors, and providing flexibility for future upgrades, such as integration with deep learning models for automated pattern detection in forensic data.

## V. RESULTS & DISCUSSION

The Mobile Forensic Toolkit was tested across multiple Android devices with varying OS versions (Android 8–13), including both rooted and non-rooted devices. Functional testing demonstrated successful detection of devices via ADB, accurate extraction of contacts, SMS, call logs, and media files, and proper generation of MD5 and SHA-256 hashes for all extracted artifacts. The parsing module correctly converted raw SQLite, XML, and JSON data into structured formats (JSON/CSV), enabling seamless reporting.

Performance analysis indicated that extraction times were acceptable for small and medium datasets, while larger media files increased processing duration. USB connection stability impacted extraction speed, requiring reconnections in certain cases. Despite these minor limitations, all modules-maintained data integrity, verified through hash comparison and logging, ensuring forensic soundness.

The toolkit's reporting functionality successfully generated court-ready PDF and HTML documents, presenting device metadata, timestamps, and artifact summaries. The intuitive GUI facilitated investigator operations, requiring minimal

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502072|

technical expertise while maintaining rigorous forensic standards. Comparatively, the toolkit offers a cost-effective alternative to proprietary forensic tools like Cellebrite UFED or Oxygen Forensic Suite, addressing common limitations such as restricted access to non-rooted devices and incomplete automated reporting.

In discussion, these results confirm that a modular, layered architecture combined with ADB-based extraction and automated parsing can achieve reliable, repeatable, and legally admissible forensic analysis. Future integration of AI-driven analytics, cloud data acquisition, and cross-platform support can further enhance accuracy, reduce investigation time, and extend usability to iOS and hybrid devices.

## VI. CONCLUSION

The Mobile Forensic Toolkit provides a comprehensive, reliable, and efficient solution for Android device forensics. It enables the successful extraction and preservation of both user and system data with cryptographic verification, ensuring the integrity of evidence. The toolkit accurately parses diverse data formats into structured, investigator-friendly outputs and generates professional, court-admissible reports complete with metadata and integrity logs. Its user-friendly interface ensures accessibility for investigators with minimal training. While minor performance limitations exist with large media files and occasional USB instability, the toolkit demonstrates strong operational effectiveness, bridging the gap between expensive commercial solutions and open-source alternatives by combining automation, integrity assurance, and detailed reporting. The research further highlights the potential for enhancements, including AI-assisted evidence prioritization, cloud and multi-device support, and automated media analysis. Overall, the toolkit represents a significant step toward accessible, reliable, and legally compliant mobile forensics.

Additionally, its modular architecture allows future feature expansion without compromising system stability or forensic soundness. The toolkit promotes standardized forensic procedures, improving consistency and repeatability across investigations. By reducing dependency on costly proprietary tools, it supports broader adoption of digital forensics in resource-constrained environments.

## REFERENCES

1. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd Edition). Academic Press.
2. Lessard, J., & Kessler, G. C. (2010). Android Forensics: Investigation, Analysis and Mobile Security for Google Android. Syngress Publishing.
3. Alasmary, W., Alhaidari, F., & Alhaidari, F. (2020). Mobile Device Forensics: Challenges and Techniques. Journal of Digital Forensics, Security and Law, 15(3), 45–60.
4. Quick, D., & Choo, K. K. R. (2014). Android Forensics: Investigation of Data Remnants on Android Devices. Digital Investigation, 11(3), 224–233.
5. Android Developers. (2025). Debugging and ADB Documentation. Retrieved from https://developer.android.com/studio/command-line/adb
6. Faruki, P., Laxmi, V., & Gaur, M. S. (2015). Android Security: A Survey of Issues, Malware Penetration, and Defences. IEEE Communications Surveys & Tutorials, 17(2), 997–1022.
7. Martini, B., & Choo, K. K. R. (2012). An Integrated Conceptual Digital Forensic Framework for Cloud Computing. Digital Investigation, 9(2), 7180.
8. Hoog, A., & Strzempka, R. (2011). Android Forensics: Investigation, Analysis and Mobile Security for Google Android. Elsevier.
9. Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. arXiv preprint arXiv:1604.08843.
10. Kruse II, W. G., & Heiser, J. G. (2001). Computer Forensics: Incident Response Essentials. Addison-Wesley Professional.
11. Zdziarski, J. (2011). iPhone Forensics: Recovering Evidence, Personal Data and Corporate Assets. O'Reilly Media.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details