REVIEW ARTICLE

International Journal of Forensic Science
Volume 8 Number 1, January - June 2025

Forensic Techniques for Android Devices Using Logical Extraction and Temporary Root Methods

Vinay Chauhan[1], Neeraj Kumar[2], Atul Kumar Tiwari[3], Dev Brat Mishra[4]

How to cite this article:

Vinay Chauhan, Neeraj Kumar, et al. Forensic Techniques for Android Devices Using Logical Extraction and Temporary Root Methods. Int Jr of Forensic Sci. 2025; 8(1): 51–55.

ABSTRACT

This paper presents a comprehensive analysis of forensic techniques for Android devices, focusing on logical extraction methods and temporary root techniques. As Android smartphones continue to dominate the mobile market, they serve as critical sources of digital evidence in forensic investigations. However, security mechanisms such as application sandboxing, encryption, and file-based access controls pose challenges to forensic data acquisition. Logical extraction techniques provide a non-intrusive approach to retrieving user-accessible data, ensuring evidence integrity while maintaining the device's operational state. This method is particularly useful for standard forensic investigations where access to unaltered, user-level data is required. Conversely, temporary root methods exploit system vulnerabilities to gain elevated privileges, allowing forensic experts to access deleted and system-level files with minimal modification to the device. This approach is essential for advanced forensic investigations requiring deeper insights into device storage structures. The paper evaluates the strengths and limitations of both methodologies, considering factors such as data accessibility, forensic soundness, and legal admissibility. Additionally, it discusses the evolving landscape of Android security, highlighting challenges introduced by encryption, cloud storage, and anti-forensic techniques. A comparative analysis underscores the importance of selecting the appropriate technique based on investigative needs and device security constraints. The findings suggest that a hybrid forensic strategy beginning with logical extraction and escalating to temporary root techniques when necessary can optimize evidence acquisition while preserving forensic

AUTHOR'S AFFILIATION:

[1] Security Researcher, M.C.A, Chandigarh University, Ludhiana, Highway, Chandigarh, Punjab 140413, India.

[2] Research Scholar, Fish Biology Research Lab, Department of Zoology, Tilak Dhari Collage, Jaunpur 222002, Uttar Pradesh, India.

[3] Associate Professor and Head, Department of Environmental Biology, Awadhesh Pratap Singh University, Rewa Madhya Pradesh 486003, India.

[4] Assistant Professor, Fish Biology Research Lab, Department of Zoology, Tilak Dhari Collage, Jaunpur 222002, Uttar Pradesh, India.

CORRESPONDING AUTHOR:

Neeraj Kumar, Research Scholar, Fish Biology Research Lab, Department of Zoology Tilak Dhari Collage, Jaunpur 222002, Uttar Pradesh, India.

E-mail: nk00267@gmail.com

➢ **Received:** 24-02-2025 ➢ **Accepted:** 04-04-2025

integrity. This study provides forensic practitioners with insights into effective Android forensic methodologies, ensuring comprehensive digital investigations within legal and ethical frameworks.

KEYWORDS

• Android Forensics • Logical Extraction • Temporary Root • Digital Evidence • Data Acquisition • Evidence Integrity

INTRODUCTION

Android devices play an integral role in contemporary digital ecosystems, functioning as essential tools for communication, social networking, entertainment, and personal data management. This widespread adoption has turned Android devices into rich sources of digital evidence, containing data critical for forensic investigations. Such data spans application logs, system files, multimedia content, and potentially recoverable deleted information, making these devices indispensable in legal and investigative contexts[1-2]. The growing reliance on Android smartphones in various domains, including corporate environments and personal communication, has significantly increased the need for effective forensic techniques[3]. Unlike traditional computing devices, Android smartphones feature unique architectures, including distinct file systems, application sandboxing, and encryption mechanisms, all of which present challenges to forensic investigations[4]. Furthermore, security enhancements introduced by Google, such as file-based encryption (FBE) and scoped storage, further complicate data acquisition efforts[5] additionally, the extensive use of messaging and social media applications, such as WhatsApp and Facebook Messenger, has introduced new challenges in forensic investigations, as these applications employ end-to-end encryption, making data retrieval complex (6). Cloud storage integration in Android devices has also shifted forensic focus toward remote data acquisition methods, requiring forensic tools capable of extracting evidence stored on cloud services like Google Drive and OneDrive[7]. Research has also indicated that different Android manufacturers implement proprietary modifications to the Android OS, further complicating forensic efforts. Device-specific implementations can introduce variations in data storage locations, encryption mechanisms, and logging structures, thereby affecting the applicability of standardized forensic tools[8]. Forensic experts must therefore adopt adaptable methodologies that cater to these variations, ensuring accurate data extraction and preservation[9]. The role of forensic practitioners is not limited to data acquisition but also extends to ensuring evidence integrity and admissibility in legal proceedings. Challenges such as anti-forensic techniques, data volatility, and legal constraints necessitate the adoption of advanced forensic frameworks that align with judicial requirements[10]. Digital forensic experts employ a combination of logical extraction and temporary root methods to overcome these challenges. Logical extraction offers a structured approach by retrieving user-accessible data without modifying the device's state, ensuring high reliability in evidence preservation[1]. In contrast, temporary root techniques enable deeper access by exploiting system vulnerabilities, allowing forensic practitioners to recover deleted and system-level files with minimal risk of data alteration [2]. Both methods serve distinct forensic objectives, and their applicability depends on the investigative context, the security constraints of the targeted device, and legal admissibility considerations[3]. As the field of Android forensics continues to evolve, the need for robust, adaptive, and legally sound methodologies remains paramount. This paper critically examines the effectiveness of logical extraction and temporary root techniques, analyzing their advantages, limitations, and practical applications within forensic investigations.

Digital forensic experts are tasked with addressing two principal challenges when working with Android devices:

1. **Accessing Complex Data Structures:** Android devices store diverse datasets across various partitions, including user data, cache, and system files. These partitions house valuable evidence but often restrict access due to security measures.

2. **Preserving Evidence Integrity:** Ensuring that data remains unaltered during extraction is paramount to its admissibility in legal proceedings. Any modification can compromise the reliability of the evidence.

The Android operating system incorporates robust security features, including sand boxing and user-permission mechanisms, that enhance privacy and security but simultaneously limit access for forensic purposes. These restrictions necessitate specialized methodologies to balance evidence accessibility with integrity.

Two approaches have emerged to address these challenges:

- **Logical Extraction Methods:** These techniques focus on acquiring user-level data without altering the device's software or security settings. Logical extraction is particularly advantageous for unrooted devices, ensuring minimal interference with device integrity.
- **Temporary Root Techniques:** By exploiting system vulnerabilities, temporary root methods enable investigators to obtain elevated privileges temporarily. This approach grants access to system-level and deleted data while avoiding the permanent modifications associated with traditional rooting.

This paper critically examines these methodologies, providing an in-depth analysis of their respective strengths, limitations, and applicability to various forensic scenarios. By exploring their practical implementations and evaluating their impact on evidence integrity, the paper aims to guide forensic practitioners in selecting the most appropriate approach based on investigative requirements.

METHOD AND METHODOLOGY

This paper examines two primary methodologies employed in Android forensics:

1. **Logical Extraction Methods:**

   Logical extraction focuses on user-level data acquisition without requiring root access. It ensures minimal interference with the device's software and security settings. Common techniques include Android Backup Analysis, SDCard Imaging, Android Forensic Logical, and commercial tools like Oxygen-Forensics. Logical extraction is particularly useful for unrooted devices, offering a non-invasive approach to forensic investigations.

2. **Temporary Root Techniques:**

   Temporary root methods leverage vulnerabilities in the Android operating system to gain temporary elevated privileges. These techniques enable comprehensive data access, including system-level and deleted files, without making permanent modifications to the device. Methods such as ZergRush, Setuid, GingerBreak, and AdbRestore are frequently used in this approach. Temporary root is ideal for advanced forensic investigations requiring deeper insights.

Logical Extraction Method

Logical extraction methods focus on obtaining data without requiring root access, ensuring minimal interference with device integrity. Techniques commonly employed include Android Backup Analysis, SD Card Imaging, Android Forensic Logical, and commercial tools like Oxygen-Forensics.

Key Techniques

- **Android Backup Analysis:** Utilizes the Android Debug Bridge (ADB) to create device backups, capturing critical application data without requiring root access. This method effectively preserves evidence integrity and retrieved the highest volume of files among the studied techniques.
- **SDCard Imaging:** Focuses on acquiring data stored on external memory. While effective for recovering external files, it cannot access internal or deleted data, limiting its utility in comprehensive forensic investigations.
- **Android Forensic Logical and Commercial Tools:** These approaches target specific file types but often require application installation, which may alter device states. For example, Android Forensic Logical captured 58 files, while Oxygen-Forensics specialized in system-level files (1).
- **Social media and Messaging Forensics**: Logical extraction has proven effective for analyzing social networking and messaging applications, such as WhatsApp. Previous research

demonstrated that logical methods could capture communication logs, shared media, and contact information without modifying the device. For instance, Android Backup Analysis can recover databases containing chats and metadata essential for forensic analysis.

Advantages

1. **Non-intrusive:** Logical extraction avoids modifying the device's software, ensuring evidence integrity.
2. **Broad Applicability:** Effective for unrooted devices, making it a versatile solution for standard investigations.
3. **Ease of Use:** Methods like Android Backup Analysis require minimal technical expertise.

Disadvantages

1. **Limited Accessibility:** Unable to retrieve deleted or system-level data.
2. **External Dependency:** Techniques like SDCard Imaging depend on the presence of external memory cards.
3. **Restricted Scope:** Focuses primarily on user-level data, leaving gaps in comprehensive forensic investigations.

Temporary Root Method

Temporary root techniques leverage Android system vulnerabilities to gain root privileges temporarily, facilitating access to the device's entire data set, including system and deleted files. Unlike permanent rooting, these methods avoid persistent modifications, reducing risks to evidence integrity.

Key Techniques

- **ZergRush:** Exploits stack overflow vulnerabilities in the libsysutils.so library.
- **Setuid:** Takes advantage of initialization flaws in older Android versions to retain root privileges.
- **GingerBreak:** Modifies the global offset table of system binaries, enabling the execution of shellcode with root access[2].
- **AdbRestore:** Manipulates temporary directories to access system-level data.

Advantages

1. **Comprehensive Data Access:** Enables retrieval of deleted and system-level data.
2. **Minimal System Impact:** Avoids permanent modifications, preserving evidence integrity.
3. **Physical Acquisition:** Facilitates creation of complete binary images for detailed analysis.

Disadvantages

1. **Technical Complexity:** Requires expertise to execute correctly, limiting accessibility for general practitioners.
2. **Device Specific Vulnerabilities:** Effectiveness depends on the availability of suitable vulnerabilities for the targeted device.
3. **Potential Risks:** While minimal, temporary modifications still introduce slight risks to evidence integrity.

Comparative Analysis

Logical extraction and temporary root methods serve distinct forensic objectives, with unique strengths and weaknesses

Table 1: Show Comparative Analysis of Logical Extraction and Temporary Root

Feature	Logical Extraction	Temporary Root
Device Modification	No	Minimal
Data Accessibility	Limited to user-level data	Comprehensive, including deleted data
Suitability	Unrooted devices	Advanced forensic investigations
Impact on Evidence	Non-invasive	Minimal but requires expertise
Universality	Broad across devices	Limited by device-specific vulnerabilities

While logical extraction is ideal for preserving evidence in standard cases, temporary root methods enable deeper insights, particularly in advanced investigations requiring deleted or system-level data.

CONCLUSION

The choice between logical extraction and temporary root methods depends on the forensic objectives, device conditions, and the scope of the investigation. Logical extraction offers a reliable and non-invasive approach for standard forensic needs, particularly when working with unrooted devices. Temporary root, on the other hand, provides a robust solution for comprehensive and advanced

forensic investigations, offering access to system level and deleted data.

A hybrid approach could be the future of Android forensics, where the investigator begins with logical extraction for quick and safe access to user-level data and transitions to temporary root methods when deeper insights are required. Such a strategy would ensure a balance between data accessibility and evidence integrity, thereby enhancing the reliability and effectiveness of forensic investigations.

Conflict of Interest: No

Funding: No

Ethics Declaration: No

REFERENCES

1. Lukito, N.Y.P., Yulianto, F.A., & Jadied, E. (2016). Comparison of Data Acquisition Techniques Using Logical Extraction Method on Unrooted Android Devices. 2016 Fourth International Conference on Information and Communication Technologies (ICoICT), 1-6. IEEE.
2. Guo, W., Wu, S., & Wang, D. (2017). A Forensic Method for Android Devices Based on the Technique of Temporary Root. The 12th International Conference on Computer Science & Education (ICCSE), 502-505. IEEE.
3. Hoog, A. (2011). Android Forensics: Investigation, Analysis, and Mobile Security for Google Android. Syngress.
4. Vidas, T., Zhang, C., & Christin, N. (2011). Toward a General Collection Methodology for Android Devices. Digital Investigation, 8, S14-S24.
5. Ableson, F., Collins, C., & Sen, R. (2009). Unlocking Android. Manning Publications.
6. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.
7. Lessard, J., & Kessler, G. (2010). Android Forensics: Simplifying Cell Phone Examinations. Small Scale Digital Device Forensics Journal, 4(1).
8. Rogers, M.K., & Seigfried, K. (2004). The Future of Computer Forensics: A Needs Analysis Survey. Computers & Security, 23(1), 12-16.
9. Stuttgen, J., & Cohen, M. (2013). Anti-Forensic Resilient Memory Acquisition. Digital Investigation, 10, S105-S115.
10. Ovens, M., & Morison, S. (2016). Forensic Examination of Mobile Devices Using Open-Source Tools. Forensic Science International, 267, 26-34.