Int. J. Advanced Networking and Applications
Volume: 17 Issue: 04 Pages: 7045-7054 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17407

Android Forensics: A Literature Review of Methodologies and Tool Efficacy

Prince Kumar
Research Scholar, Faculty of Computing & IT, UMU Ranchi
Email: kprince87@gmail.com
Dr. Ritushree Narayan
Assistant Professor, Faculty of Computing & IT, UMU Ranchi
Email: ritushree@umu.ac.in
Dr. Ekbal Rasid
Professor, St. Peter's Engineering College, Hyderabad
Email: ekbalrashid2004@yahoo.com

ABSTRACT

The rapid growth of Android smartphone usage has significantly increased the importance of Android mobile forensics in cybersecurity. This paper presents a comprehensive review and a novel comparative performance analysis of methodologies, tools and challenges in Android applications forensics, synthesizing 25 peer reviewed studies published between 2015 and 2025. This review details current practices in data acquisition and provides an in depth, interpretative evaluation of the performance of widely used forensic tools (Magnet Axiom, Belkasoft X, Andriller, AFLogical, Autopsy, etc.) based on key recovery metrics. Our findings quantitatively demonstrate that no single tool provides complete coverage across all acquisition and analysis scenarios. The review also explores critical limitations, including device fragmentation, encrypted cloud storage, anti-forensic tactics and legal admissibility concerns. Furthermore, we discuss emerging trends such as emulator driven dynamic analysis, AI assisted examination and blockchain enhanced evidence integrity. The novelty of this research lies in its synthesis of a performance benchmark from fragmented literature and its critical analysis of tool efficacy, providing a clear, actionable guide for practitioners. This study serves as a comprehensive reference for practitioners and researchers, highlights established best practices and proposes future directions to improve investigative technology for Android forensics.

Keywords - **Android Forensics, Anti Forensic Techniques, Encrypted Data Extraction, Forensic Techniques, Forensic Tools, Literature Review.**

Date of Submission: October 30, 2025 Date of Acceptance: December 16, 2025

1. INTRODUCTION

The Mobile forensics is about finding, studying and saving digital evidence from mobile devices. Because so many people use smartphones, the mobile forensic has become very important for criminal investigations, cybersecurity and protecting companies [1]. Studying mobile devices is often harder than studying computers. This is because phone software updates often, the hardware is very different between models and many messaging apps use strong encryption that locks the data [2]. Getting data from cloud storage is also difficult and often requires legal permission [3]. The field also deals with "anti-forensic" techniques used by cyber criminals. They use tools to hide their data, apps to delete it securely and encrypted platforms to communicate. Obfuscation tools change or hide data to make forensic analysis hard. Some harmful software uses code that changes itself every time it runs to avoid being found [4]. Because these threats are always changing, forensic methods must also keep changing to make sure the evidence collected is trustworthy [5]. Android and iOS are the two main types of smartphones. Each one has its own challenges for forensics because they have different security, encryption and designs [3, 14]. This study focuses on Android. We chose Android because it is the most used phone in the world, with about 74% of the market as of June 2025, while iOS has 25% (Stat Counter, 2025) as seen in fig 1.

Because Android is so common, it is often part of investigations. Also, Android is "open source," which means researchers can look at its code to build better forensic tools. But it is harder to do with a closed system like iOS [5]. The fig 2 shows the comparative analysis of android and iOS.

Because many different companies make Android phones which creates special challenges that need flexible solutions.

The constant changes in mobile security and digital privacy create ongoing problems for forensic investigations [6]. Many older forensic tools cannot get or analyze data from new Android devices well. The natural difficulty of getting forensic data has led to continuous discussion about the best methods, tools and new trends [5]. Doing a Literature Review can give us useful information about current

Volume: 17 Issue: 04 Pages: 7045-7054 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17407

methods and the problems experts face [7]. Looking at existing research can also show which parts of forensic methods need more work and improvement.

This research aims to review the methodologies and tools used in mobile forensic investigations with a specific focus on Android forensics. This focused approach lets us investigate the specific techniques, tools, challenges and limits of the Android platform. To explore these areas, our study is guided by the following research questions:

- RQ1: What are the common methods and tools used to get digital evidence from Android devices with focusing on main problems and limits faced when analyzing Android?
- RQ2: How do new Android features, like better security and encryption, affect forensic investigations and what are the new trends and future directions in Android mobile forensics?

2. BACKGROUND

An evaluation of Android Forensics methodologies and tools reveals a number of advances that reflect the dynamic nature of technology and the challenges in forensic investigations. Recent studies highlight significant progress in the classification of mobile forensic tools [8]. These tools cover a variety of data extraction techniques, essential for accessing volatile and non-volatile memory in Android smartphones. Methodologies such as logical extraction, physical extraction and file system analysis emerged as fundamental approaches in capturing digital evidence. Each method has advantages and limitations due to the growing complexity of mobile applications. However, the rapid growth of technology it introduces a set of challenges that complicate forensic efforts. As Ghaffari (2025) point out that updates and variations in the operating system in application compilation can significantly limit the effectiveness of current methodologies [9]. Android device fragmentation which caused by manufacturers' OS modifications, complicates forensics. This demands flexible methodologies to effectively recover and analyze data across diverse devices. The field of Android mobile forensics faces challenges that directly impact data recovery and its admissibility in legal proceedings. A primary obstacle is the use of encryption by both device manufacturers and application developers. Which creates a significant barrier for forensic experts attempting to extract information, potentially rendering evidence inadmissible in court [10,11]. Further complexities arise from the continuous evolution of malware designed to obstruct analysis [12], the extreme fragmentation of Android devices across manufacturers [13] and rapidly changing application permissions and privacy policies that complicate evidence collection within legal and ethical boundaries [14]. There is a growing emphasis on real time analysis to improve threat detection and preserve data integrity during investigations [15]. Concurrently, researchers advocate for the development of comprehensive frameworks to systematize mobile forensic processes [16]. The creation of standardized protocols to address inconsistencies and improve data recovery outcomes for legal processes [17]. Looking forward, the integration of artificial intelligence (AI) presents a promising avenue for streamlining data analysis and enhancing investigative capabilities. However, the adoption of AI introduces its own set of challenges, including concerns over algorithmic bias, transparency and the interpretation of results in a legal context [18, 19]. The rapid evolution of mobile technology underscores an urgent need for continuous methodological updates to develop robust forensic practices that maintain the integrity of digital evidence.

2.1 Digital Forensics and Mobile Forensics Foundations

Digital forensics is a careful process of finding, examining and showing electronic information as evidence [20]. It has different branches, like computer, network, cloud and mobile forensics. Each branch uses its own special tools and methods. In mobile forensics, investigators look for specific pieces of data. This includes text messages, call logs and information from apps, like chat histories, photos and details about that data [21]. For example, messaging apps often save user information in their own special database formats. To read this data, investigators often need to decrypt it or figure out how the app works, which can be difficult [22].

Even though the methods vary between these branches, the main process usually has four key steps [20]:

- Identification: Finding and recording where potential evidence is stored. On a mobile device, this could be the phone's internal memory, a removable SD card, data synced to the cloud, or app logs.
- Acquisition: Carefully copying the data without changing it. The method used depends on things like the level of encryption, the phone's software version and what forensic tools are available.
- Analysis: Looking closely at the collected data to find important evidence. Investigators go through call histories, messages, installed apps, network connections and location records. They often need special keys to unlock data or extra software tools to understand app files and find deleted items [23].
- Presentation: Putting the findings into a clear report that can be used in court or in a company. The report explains the tools and methods used, who handled the evidence and why the discovered information is important. This allows courts or company leaders to trust the evidence [1].
- These steps show why a clear and repeatable process is needed. This is especially true in mobile forensics, where different devices can make things complicated. Following this process is essential to make sure the digital evidence is trustworthy, correct and useful for legal or business decisions [1].

Volume: 17 Issue: 04 Pages: 7045-7054 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17407

2.2 Data Acquisition Techniques in Android Forensics

Android is popular due to its open source nature. However, this also leads to a "fragmented" ecosystem with many different device makers, hardware parts and security systems. Because of this, a forensic method that works on one Android model or version might not work on another. Investigators must change their approach for different devices. In Android investigations, four main techniques are used to get data. Each one gives a different level of access to files, deleted records and encrypted information:

- Physical Acquisition: It makes a bit-by-bit copy of the entire device's storage. This can recover deleted files and hidden areas. It gives the most data but it often requires to bypass the strong security features which can be very difficult on new devices [5].
- Logical Acquisition: This technique uses special software to copy the data you can normally see on the device [20]. It is easier and less invasive but cannot recover deleted files or data locked by strong encryption. Common tools like Magnet AXIOM, Belkasoft X and Cellebrite UFED use this method.
- File System Acquisition: This method specifically targets the organized structure of files and folders on the device [27]. It lets analysts capture detailed information about files, app folders and databases.
- Cloud Based Acquisition: Since many Android apps automatically back up data to the cloud (like Google Drive), investigators often need legal permission to get this remote data [3]. Challenges include multi factor authentication and the risk that a user could delete the data remotely. However, cloud data can provide very useful information from past backups and synced account details.

2.3 Challenges in Android Forensics

Latest Android devices usually uses strong encryption (called Advanced Encryption Standard or AES) to protect the user’s data. The keys for this encryption are often managed by the device's hardware, making them very hard to get [28]. When combined with other security features, these measures make it very difficult to acquire forensic data, especially if the device is protected with a strong password or a fingerprint/face scan.

- End to End Encryption in Messaging Apps: Apps like WhatsApp and Signal use "end to end encryption." This means messages are scrambled so that only the sender and receiver can read them [18]. Because of this, forensic examiners cannot simply read the messages from the company's servers. They must instead try to find copies of the data (cached files) stored locally on the device or look in the device's temporary memory.
- Anti Forensic Tactics: People trying to hide their activities use different methods to avoid detection:
- Secure Deletion Tools: These are apps designed to permanently erase data by overwriting it many times, making it impossible to recover with standard forensic tools [29].
- Obfuscation Methods: These are tricks to hide data. For example, they might hide information inside a normal looking picture (steganography) or scramble it with special codes (XOR encoding) or multiple layers of encryption [30, 31].
- Rooted Devices and Custom ROMs: If a user "roots" their Android device or installs a custom operating system (like LineageOS), they get high level control over the system. This lets them delete or change evidence more easily [35]. In these situations, investigators need very specialized, device specific methods to get the data accurately and in a way that will be accepted in court.

2.4. Emerging Trends in Mobile Forensics

New developments are starting to use artificial intelligence (AI), blockchain and Internet of Things (IoT) technologies.

- AI methods, like machine learning, can help sort through huge amounts of data much faster and more accurately, though human experts are still essential to check the results [36].
- Blockchain technology can create a very secure and unchangeable record for the "chain of custody," proving that evidence was not tampered with [37].
- The growth of IoT devices (like smartwatches and home assistants) creates new sources of evidence but also new challenges, requiring forensic tools and methods to adapt [38]. Current trends, such as using blockchain and "fog computing," show potential for dealing with the complexities of modern investigations [39].

In summary, this chapter has explained the basic ideas, the forensic process models, the data acquisition techniques, the main challenges and the new trends that are the foundation of mobile forensics, with a special focus on Android. This background information will help guide the methodology, tool evaluations and discussions that are the main part of this review.

3. METHODOLOGY

This section explains the step by step process used for this study. It details how the literature review was done, including the search plan, how studies were chosen and how their quality was checked. This structured method ensures the review of existing research is thorough and fair, reducing bias and making the findings more reliable. It uses a three phase flow (Planning → Conducting → Reporting) to mirror the structure of a Literature Review as fig 1.

Volume: 17 Issue: 04 Pages: 7045-7054 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17407

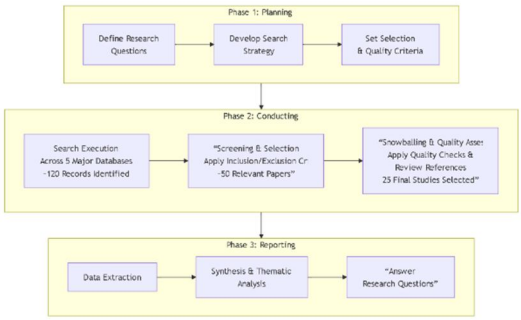

Fig 3: Literature Review Methodology

3.1 Research Method

This study uses a Literature Review following well known guidelines [7]. A literature review (LR) is a method for carefully finding, selecting and analyzing all relevant research on a topic. It uses a clear and repeatable process to reduce bias and make the conclusions more trustworthy [7, 5]. The LR process has three main phases:

- Planning the review: Deciding on the research questions and creating a plan for how to search for studies.
- Conducting the review: Doing the search, picking out the relevant studies and collecting the needed information from them.
- Reporting the findings: Summarizing and analyzing the results to find trends, challenges and areas that need more research.

3.2 Search Strategy

A wide search was done across several online databases to find relevant, high quality studies on mobile forensics, with a special focus on Android devices.

- Databases Used: The search included IEEE Xplore, ACM Digital Library, Elsevier ScienceDirect, SpringerLink and Scopus.
- Search Terms: A mix of keywords and connectors (like AND/OR) was used. Terms included: "Android mobile forensics," "Android digital forensics," "data acquisition in Android forensics," "forensic tools for Android," and "challenges in Android mobile forensics." Different wordings and synonyms were also tried. The lists of references in key papers were also checked to find more studies.
- Example Search String: (intitle:"android forensics" OR "Android mobile forensics" OR "Android digital forensics" OR "Data acquisition in Android forensics") AND (filetype:pdf OR filetype:docx)

3.3 Selection Criteria

Specific rules were set to include only high quality and relevant studies.

Inclusion Criteria:

- Studies published between 2015 and 2025.
- Peer reviewed journal articles and conference papers.
- Studies focused on mobile forensics, specifically Android devices.
- Papers discussing forensic tools, methods, data acquisition techniques and challenges.

Exclusion Criteria:

- Non peer reviewed sources (e.g., blogs, non-academic reports).
- Studies not focused on mobile device forensics.
- Duplicate papers or those that didn't add substantial knowledge.
- Papers not written in English or Spanish.

3.4 Quality Assessment

A quality check was done to ensure the selected studies were reliable and valid. This was based on:

- Relevance: How directly the study related to Android mobile forensics and our research goals.
- Methodological Rigor: How well the study was designed and conducted.
- Transparency: How clearly the study explained its methods, data and any limitations.

The Selection Process in Action:

The search started with about 120 papers. After applying the rules above, this list was reduced to about 50 papers. Then, the "snowballing" technique (looking at the references in these papers and who cited them) found over 130 more documents. After applying the same filters and quality checks again, a final list of 25 high quality papers was selected to form the core of this review.

3.5 Data Extraction and Synthesis

For each of the 25 selected studies, the following information was collected:

- Basic details (title, authors, year, source).
- The study's main goals and scope.
- The forensic techniques it discussed (methods, tools).
- Its key findings (challenges, limitations, new trends).
- Its suggestions for future research.

3.6 Analysis of Selected Papers

The final 25 papers were compared and analyzed based on the two research questions (RQ1, RQ2). The information was grouped into categories like methods, tools and challenges. Studies were sorted by which research question they best addressed. This process helped identify common patterns, agreements, differences and new trends, making the final conclusions stronger.

Volume: 17 Issue: 04 Pages: 7045-7054 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17407

4. RESULTS & DISCUSSION

This section presents the key findings from the analysis of the selected studies, organized by the research questions. The results provide a comprehensive overview of the current landscape, prevailing practices and emerging trends in Android forensic investigations.

4.1 Common Forensic Methods and Tools for Android Evidence Acquisition

The systematic review of literature reveals several established methodologies for acquiring digital evidence from Android devices, each with distinct advantages and limitations.

4.1.1 Primary Acquisition Techniques

- Logical acquisition emerges as the most accessible approach, utilizing standard Android interfaces such as Android Debug Bridge (ADB) to extract filesystem visible data [39]. While this method preserves forensic soundness through its non-invasive nature, its fundamental limitation lies in the inability to recover deleted content or access encrypted partitions [41].
- Physical acquisition represents the gold standard for evidence completeness, creating sector by sector copies of device storage that enable recovery of deleted artifacts and unallocated space [40]. However, this technique faces significant barriers in modern Android ecosystems, particularly against hardware backed encryption and locked bootloaders that often require root access, potentially compromising evidence admissibility [42].
- File system acquisition occupies an intermediate position, providing detailed metadata and application specific artifacts while remaining constrained by the same encryption limitations that affect logical methods [52].

4.1.2 Specialized and Emerging Methods

The evolving forensic landscape has necessitated complementary approaches:

- Cloud based acquisition addresses the paradigm shift toward distributed data storage, though it introduces jurisdictional complexities and dependency on provider cooperation [43]
- Memory imaging captures volatile RAM contents, potentially revealing decryption keys and ephemeral application states [44]
- Dynamic analysis frameworks such as AnForA automate behavioral monitoring in emulated environments, establishing causal relationships between user actions and digital artifacts [52]

4.1.3 Forensic Tool Ecosystem

The tool landscape bifurcates into commercial and open-source solutions, each serving distinct investigative contexts:

Table 1: Comparative Analysis of Android Forensic Tools

Tool Category	Representative Tools	Primary Strengths	Notable Limitations
Logical Acquisition	ADB, AFLogical, Magnet Acquire	Forensic soundness, accessibility	Limited to active filesystem data
Physical Acquisition	Cellebrite UFED, Dr.Fone, Andriller	Deleted data recovery, comprehensive imaging	Root requirements, legal concerns
Analysis Platforms	Belkasoft X, Autopsy, Oxygen Forensic	Multi source correlation, reporting	Encrypted data handling, device support variability
Specialized Frameworks	Fordroid, AnForA, Argus	Automated analysis, behavioral tracking	Laboratory constraints, setup complexity

4.2 Performance Evaluation and Interpretation of Forensic Tools

This section provides a critical analysis and interpretation of forensic tool performance based on synthesized data from comparative studies.

4.2.1 Interpretation of Comparative Data Recovery (Table 2)

The Table 2 presents aggregated recovery metrics from controlled experiments reported in the literature [48, 53]. The interpretation of this data reveals strategic strengths and weaknesses:

- Magnet AXIOM excelled in recovering documents (11,957) and a high volume of pictures (61,193), indicating superior parsing capabilities for common file systems and file carving. This makes it highly effective for investigations focused on document trails and multimedia evidence.
- Belkasoft X demonstrated strong performance in parsing chat data (1,533) and enumerating installed apps (611), suggesting advanced support for application artifacts and databases. Its ability to locate encrypted files (228) is a distinct advantage for identifying potential evidence barriers.
- Autopsy, while a powerful open-source tool, showed lower courts across most metrics. This often reflects its reliance on community developed modules and potentially less out of the box support for proprietary app formats compared to commercial suites. However, its extensibility and

Volume: 17 Issue: 04 Pages: 7045-7054 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17407

cost make it a vital tool for foundational analysis and verification.

Key Interpretation: The data is not a declaration of a "best" tool, but a map of contextual efficacy. An investigation into financial fraud might prioritize Magnet AXIOM for document recovery, while a case involving encrypted messaging would benefit from Belkasoft X's chat and encryption awareness. The novelty of this synthesis is that it transforms isolated study results into a comparative benchmark, allowing practitioners to make evidence-based tool selections.

4.2.2 Holistic Tool Evaluation: Beyond Raw Data

Performance extends beyond recovery counts. Table 3 (from the original manuscript) integrates critical operational and legal dimensions:

- Forensic Soundness vs. Practicality: Tools like ADB and Magnet Acquire offer high forensic soundness (low risk of alteration) but are limited to logical extraction. Tools enabling physical acquisition (e.g., Andriller, Dr.Fone) often require root access, which can alter the device and challenge legal admissibility.
- The Usability Automation Trade off: Commercial tools (Belkasoft X, Magnet AXIOM) offer GUI driven automation, significantly reducing analysis time. Framework based tools (AnForA, Argus) offer deep behavioral insights but require extensive setup and expertise.
- Legal Admissibility: Tools that provide robust chain of custody logging, hash verification and output in forensically sound formats (e.g., E01) are essential. The claim that data from root dependent tools remains "admissible" requires careful validation against jurisdictional standards.

4.2 Critical Challenges in Android Forensic Analysis

The implementation of these methodologies confronts substantial obstacles that define the current boundaries of Android forensics.

4.2.1 Technical and Ecosystem Barriers

Device and OS fragmentation constitutes a fundamental challenge, with heterogeneous hardware architectures, filesystems and manufacturer implementations necessitating device specific acquisition approaches [42]. This fragmentation effectively precludes universal forensic solutions, demanding continuous tool adaptation and investigator training [45].
Encryption technologies have dramatically altered the forensic landscape. Full disk encryption (FDE) and file based encryption (FBE), when coupled with hardware security modules, render traditional acquisition methods ineffective against contemporary devices [42, 49]. The proliferation of end to end encryption (E2EE) in messaging applications further obscures communication evidence, restricting analysts to cached artifacts or memory forensics [47].

4.2.2 Anti Forensic and Procedural Challenges

Anti forensic techniques actively subvert investigative efforts through multiple vectors:

- Data hiding via steganography and encrypted containers [46]
- Artifact wiping through secure deletion applications [52]
- Trail obfuscation using timestamp manipulation and data fragmentation [50]
- Legal and ethical constraints introduce procedural complexities, where technically feasible methods may violate privacy regulations or evidence handling protocols. The root access frequently required for physical acquisition potentially compromises forensic soundness and evidentiary admissibility [39, 42].

4.3 Impact of Android Security Evolution and Emerging Directions

4.3.1 The Encryption Imperative: Shifting Forensic Paradigms

The strengthening of Android's security architecture has fundamentally redefined forensic possibilities. Hardware backed encryption keys bound to secure hardware elements effectively nullify brute force attacks against device encryption [42]. Verified Boot mechanisms prevent the execution of modified bootloaders or custom recoveries, closing traditional acquisition pathways [49].
This cryptographic hardening has precipitated a strategic shift from device centric to ecosystem centric investigations. With local data increasingly inaccessible, forensic emphasis moves toward:

- Cloud service evidence acquisition [50]
- Peripheral device analysis (wearables, IoT companions) [52]
- Network traffic correlation and metadata analysis [50]

The novelty of this review's discussion lies in connecting these technical challenges directly to the interpreted tool performance. For instance, the prevalence of encryption (FDE, FBE, E2EE) explains why tools like Belkasoft X, which actively identify encrypted containers, are becoming more critical. Similarly, device fragmentation is the root cause why no single tool performs best across all studies each experiment may use a different device profile.

4.4 Emerging Trends and Future Directions

The field is evolving to address these challenges

- AI enhanced analysis demonstrates promising applications in pattern recognition across massive datasets, though human oversight remains critical

Volume: 17 Issue: 04 Pages: 7045-7054 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17407

for contextual interpretation [46]. Machine learning algorithms show particular utility in identifying relevant artifacts within extensive application data and detecting obfuscated content [42].

- Blockchain based evidence integrity frameworks offer tamper evident documentation of the forensic chain of custody, creating cryptographically verifiable audit trails from acquisition through courtroom presentation [48].
- Automated dynamic analysis platforms represent a paradigm shift from static artifact examination to behavioral reconstruction. By executing applications in instrumented environments, tools like AnForA systematically map user interactions to digital traces, addressing the growing challenge of application-level encryption [49].

Table 2: Comparative Analysis of data recovery

Metric	Autopsy	Belkasoft X	Magnet AXIOM
Pictures Recovered	56,480	42,736	61,193
Videos Recovered	358	588	550
Chats Parsed	624	1,533	1,270
Documents Parsed	3,741	2,395	11,957
Encrypted Files Located	–	228	–
Installed Apps Enumerated	298	611	690

4.3.3 Future Research Directions

The reviewed literature identifies several critical pathways for advancing Android forensics:

- Standardized validation frameworks for forensic tool performance across diverse device configurations
- Cross platform correlation methodologies synchronizing evidence from devices, cloud services and IoT ecosystems
- Legal technical harmonization developing investigative techniques that simultaneously satisfy technical feasibility and legal admissibility requirements
- Anti forensic capabilities proactively detecting and countering evidence obfuscation techniques

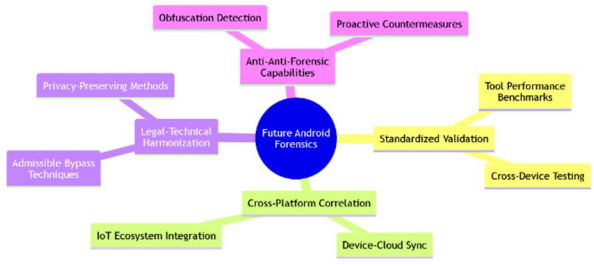

Fig 4: Future Research Directions Mind Map

The convergence of these approaches points toward an integrated future forensic workflow combining automated evidence collection, intelligent analysis prioritization and cryptographically assured evidence preservation throughout the investigative lifecycle.

Table 3: main considerations across tools.

Tool	Forensic soundness	Usability / automation	Legal admissibility
ADB Backup	Logical and non invasive	Scriptable, free, but slow (around 2 h)	Low risk (no root)
Magnet Acquire	Logical and non invasive	GUI based; fast logical extraction	Low risk (no root)
FTK Imager	Physical mode; may alter system	GUI dependent; time consuming	Potential risk (system alter ation)
Andriller	Partial physical; often root dependent	Mid level runtime; CLI/GUI options	Risk (root may compromise evidence)
Belkasoft X	Least intrusive acquisition first; chain of custody hashing	Very fast (around 10 min) com mercial UI	Built in hash and task logs for courtroom chain of custody
Dr.Fone	Requires device root for deep recovery (system modified)	Wizard UI; step by step export and recovery	Vendor claims data remains admissible in court
DiskDigger	Full scan needs root; risk to integrity	Basic scan seconds; deep scan minutes	No documented courtroom validation
Recover My Files	Forensic Imager creates sector level DD/AFF/E01 with hashes	Wizard workflow; event log and progress	E01 format widely accepted as evidence

5. LIMITATIONS

- Internal Validity: Our search relied on academic databases and sources in English and Spanish. This means we might have missed some relevant "gray literature" (like reports from companies or governments). There is also a small risk of subjective judgment when interpreting how rigorous a study's methods were. Also, our evaluation of tools is based on other published studies, which might contain the original authors' own biases.
- Construct Validity: Our assessment of how well tools perform is based on findings from other comparative studies, not on our own direct testing. This could lead to inconsistencies because the original studies were done under different test conditions.
- Conclusion Validity: We followed a clear, documented process to make sure studies were selected and data was extracted consistently. Multiple reviewers were involved to reduce personal bias and any disagreements were solved through discussion.

Volume: 17 Issue: 04 Pages: 7045-7054 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17407

- External Validity: Our findings are mostly based on academic and laboratory scenarios. We must be careful about applying them directly to real world investigations, because practical, legal and geographical factors can change the outcome in ways this review does not capture.

6. CONCLUSIONS AND FUTURE WORK

This Literature Review has combined current research to show the state of Android mobile forensics today. It looked at the methods, tools, challenges and how well they work. The analysis shows a clear trend towards using "hybrid" methods. These methods combine different types of analysis to deal with the growing complexity caused by:

- Many different Android devices.
- Strong encryption.
- Techniques used to hide or destroy evidence.

While commercial tools (like Magnet Axiom and Belkasoft X) are advanced and open-source tools (like Autopsy) are still very important, no single tool can do everything. Because of this, investigators must often use a combination of tools to get the best results.

Major challenges still remain in:

- Getting data from the cloud.
- Fighting against anti forensic techniques.
- Making sure evidence is collected in a way that is acceptable in court.

For the future, work should focus on:

- Creating standard rules to check that forensic tools work correctly.
- Getting better at defeating anti forensic measures.
- Improving and making better use of new methods, like tools that use emulators (AnForA) and static analysis (Fordroid).
- Encouraging teamwork between technology experts and legal experts. This ensures that the tools being developed meet the standards required for evidence in court.

This review provides a basic reference guide for forensic experts and researchers. It highlights the importance of tools that can work together, are updated regularly and are properly tested. This is essential to keep up with the changing demands of Android forensic investigations.

REFERENCES

[1] Adelstein, F. (2006). Live forensics: Diagnosing your system without killing it first. Communications of the ACM, 49(2), 63–66.

[2] Al Dhaqm, A., Abd Razak, S., Ikuesan, R. A., Kebande, V. R., & Siddique, K. (2020). A review of mobile forensic investigation process models. IEEE Access, 8, 173359–173375.

[3] Alatawi, H., Alhazmi, E., Alsubhi, K., & Alzahrani, A. (2020). Mobile forensics: A review. In Proceedings of the International Conference on Computer and Information Technology (ICCIT) (Vol. 2, pp. 1–6).

[4] Almuqren, L., Alsuwaelim, H., Rahman, M. M. H., & Ibrahim, A. A. (2024). A systematic literature review on digital forensic investigation on android devices. Procedia Computer Science, 235, 1332–1352.

[5] Android Open-Source Project. (2023). Full disk encryption. https://source.android.com/security/encryption

[6] Anglano, C. (2014). Forensic analysis of whatsapp messenger on android smartphones. Digital Investigation, 11(3), 201–213.

[7] Anglano, C., Canonico, M., & Guazzone, M. (2020). The android forensics automator (anfora): A tool for the automated forensic analysis of android applications. Computers & Security, 88, 101650.

[8] Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013). A critical review of 7 years of mobile device forensics. Digital Investigation, 10(4), 323–349.

[9] Bennett, J. L. (2013). The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations. Forensic Science International, 231(1-3), 130–135.

[10] Bernardo, B. M. V., Mamede, H. S., Barroso, J. M. P., & dos Santos, V. M. P. D. (2024). Mobile device forensics framework: A toolbox to support and enhance this process. Emerging Science Journal, 8, 972–998.

[11] Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. International Journal of Digital Evidence, 2(2).

[12] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

[13] Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017). Mobile forensics: Advances, challenges and research opportunities. IEEE Security & Privacy, 15(6), 42–51.

[14] Cristian, P. C., Hernan, T. C., Rene, G. Q., Francisco, A. P., & Cristian, N. G. (2020). Methodologies and forensic analysis tools on android mobile devices: A systematic literature review. In 2020 15th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1–7). IEEE.

[15] Ehsan, M., Catal, C., & Mishra, A. (2022). Detecting malware by analyzing app permissions on android platform: A systematic literature review. Sensors, 22(20), 7928.

Volume: 17 Issue: 04 Pages: 7045-7054 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17407

[16] Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M. (2015). Android security: A survey of issues, malware penetration and defenses. IEEE Communications Surveys & Tutorials, 17(2), 998–1022.

[17] Fernando, V. (2021). Cyber forensics tools: A review on mechanism and emerging challenges. In 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1–7). IEEE.

[18] Garfinkel, S. L., & Shelat, A. (2003). Remembrance of data passed: A study of disk sanitization practices. IEEE Security & Privacy, 1(1), 17–27.

[19] Georgokitsos, K. (2018). Mobile device forensics: Guidelines, analysis and tools [Master's thesis, University of Piraeus].

[20] Harris, R. (2006). Arriving at anti-forensics' consensus: Examining how to define and control the anti-forensics problem. Digital Investigation, 3, S44–S49.

[21] Hoog, A. (2011). Android forensics: Investigation, analysis and mobile security for Google Android. Elsevier.

[22] Jeyaseeli, J. A. M., & Shanthi, C. (2022). A smart technique to extract the deleted data form the android application. International Journal of Health Sciences, 6(S1), 2864–2871.

[23] Khubrani, H. (2023). Mobile device forensics, challenges and blockchain based solution. In Proceedings of the 2nd International Conference on Smart Technologies for Smart Nation.

[24] Khubrani, H. (2024). Mobile device forensics, challenges and solutions. In Proceedings of the International Conference on Digital Forensics and Cybersecurity.

[25] Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering (Technical Report EBSE 2007-001). Keele University and University of Durham.

[26] Kitsaki, T. I., Angelogianni, A., Ntantogian, C., & Xenakis, C. (2018). A forensic investigation of android mobile applications. In *Proceedings of the 22nd Pan-Hellenic Conference on Informatics (PCI)* (pp. 1–8).

[27] Konduru, Y., Mishra, N., & Sharma, S. (2018). Acquisition and analysis of forensic data artefacts of some popular apps in android smartphone. In *2018 IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, 16th International Conference on Pervasive Intelligence and Computing, 4th International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (pp. 86–93). IEEE.

[28] Lessard, J., & Kessler, G. C. (2010). Android forensics: Simplifying cell phone examinations. Small Scale Digital Device Forensics Journal, 4(1), 1–12.

[29] Lin, X., Chen, T., Zhu, T., Yang, K., & Wei, F. (2018). Automated forensic analysis of mobile applications on android devices. Digital Investigation, 26, S59–S66.

[30] Lwin, H. H., Aung, W. P., & Lin, K. K. (2025). Comparative analysis of android mobile forensics tools. In Proceedings of the International Conference on Computer Systems and Technologies (pp. 1–8).

[31] Maček, N. D., Štrbac, P., Čoko, D., Franc, I., & Bogdanoski, M. (2016). Android forensic and anti-forensic techniques – a survey. In Proceedings of the 8th International Conference on Business Information Security (BISEC).

[32] McKemmish, R. (1999). What is forensic computing? Trends and Issues in Crime and Criminal Justice, 118, 1–6.

[33] Musa, A., & Mirza, A. (2022). Current trends in internet of things forensics. In 2022 International Conference on Cyber Security and Internet of Things (ICSIoT) (pp. 1–5). IEEE.

[34] Mutawa, N. A., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. Digital Investigation, 9, S24–S33.

[35] Mykhaylova, O., & Fedynyshyn, O. (2024). Person of interest detection on mobile forensics. In Proceedings of the International Conference on Advanced Technologies and Applications in Mobile Forensics.

[36] Ogazi-Onyemaechi, B. C., Dehghantanha, A., & Choo, K. K. R. (2017). Performance of android forensics data recovery tools. In A. Dehghantanha & K. K. R. Choo (Eds.), Contemporary digital forensic investigations of cloud and mobile applications (pp. 91–110). Elsevier.

[37] Padmanabhan, R., Lobo, K., Ghelani, M., Sujan, D., & Shirole, M. (2016). Comparative analysis of commercial and open-source mobile device forensic tools. In Proceedings of the IEEE Conference (pp. 1–6).

[38] Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding—a survey. Proceedings of the IEEE, 87(7), 1062–1078.

[39] Quick, D., & Choo, K. K. R. (2014). Google drive: Forensic analysis of data remnants. Digital Investigation, 10(1), 3–18.

[40] Raji, M., Wimmer, H., & Haddad, R. J. (2018). Analyzing data from an android smartphone while

Volume: 17 Issue: 04 Pages: 7045-7054 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2025.17407

comparing between two forensic tools. In Proceedings of SoutheastCon 2018.

[41] Riadi, I., Fadlil, A., & Fauzan, A. (2018). A study of mobile forensic tools evaluation on android based line messenger. International Journal of Advanced Computer Science and Applications (IJACSA), 9(10), 201–206.

[42] Roy, N. R., Khanna, A. K., & Aneja, L. (2016). Android phone forensic: Tools and techniques. In 2016 International Conference on Computing, Communication and Automation (ICCCA).

[43] Sathe, S. C., & Dongre, N. M. (2018). Data acquisition techniques in mobile forensics. In 2018 2nd International Conference on Inventive Systems and Control (ICISC) (pp. 280–285). IEEE.

[44] Scrivens, N., & Lin, X. (2017). Android digital forensics: Data, extraction and analysis. In *Proceedings of the ACM Turing Celebration Conference - China (ACM TUR C '17)* (pp. 1–6).

[45] Scientific Working Group on Digital Evidence. (2020). SWGDE best practices for mobile device forensic analysis (Technical Report). National Institute of Standards and Technology.

[46] Sutter, T., Kehrer, T., Rennhard, M., Tellenbach, B., & Klein, J. (2024). Dynamic security analysis on android: A systematic literature review. IEEE Access, 12, 57261–57287.

[47] Tayeb, H. F., & Varol, C. (2019). Android mobile device forensics: A review. In Proceedings of the IEEE Conference (pp. 1–8).

[48] Vasilaras, G., Papadoudis, N., & Rizomiliotis, P. (2024). Artificial intelligence in mobile forensics: A survey of current status, a use case analysis and AI alignment objectives. Forensic Science International: Digital Investigation, 49, 301737.

[49] V. Baryamureeba & F. Tushabe. (2004). The enhanced digital investigation process model. In Proceedings of the Digital Forensic Research Workshop (DFRWS).

[50] Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). Network and device forensic analysis of android social-messaging applications. Digital Investigation, 14, S77–S84.

[51] Zhang, J., E, C., & Hu, A. (2018). A method of android application forensics based on heap memory analysis. In 2018 2nd International Conference on Computer Science and Application Engineering (CSAE) (pp. 1–6).

[52] Zhang, X., Breitinger, F., Luechinger, E., & O'Shaughnessy, S. (2021). Android application forensics: A survey of obfuscation, obfuscation detection and deobfuscation techniques and their impact on investigations. Forensic Science International: Digital Investigation, 37, 301285.

BIOGRAPHIES

Prince Kumar is a research scholar in the Faculty of Computing and Information Technology, Usha Martin University (UMU), Ranchi. He obtained his Master's degree in Cyber Forensics and Information Security from the University of Madras. His research interests include self-destructing messages, Android forensics, and secure backend integration using Firebase and encryption protocols. Prince also holds a certification in Linux and actively researches open-source tools for data extraction and security testing. He has presented international conference papers and is engaged in research pertaining to secure mobile applications.

Dr. Ritushree Narayan Presently serving as an Assistant Professor in the Faculty of Computing and Information Technology at Usha Martin University, Ranchi, Dr. Ritushree Narayan brings with her over 20 years of professional experience. In Computer Science, she also earned her doctorate from Bundelkhand University. Her research interests revolve around Computational Biology, Bioinformatics, and Wireless Sensor Networks. A research-oriented person with a teaching profession, she is an active mentor to students and contributes to the academic development of IT and engineering education.

Dr. Ekbal Rashid is currently holding the position of Professor in the Department of Computer Science and Engineering at St. Peter's Engineering College in Hyderabad. He brings more than 20 years of academic and research experience to the table. Another honor in his replete career includes completing a Post-Doctoral Fellowship in Computational and Applied Mathematics from the Technical University of Sofia, Bulgaria, under the almighty supervision of Prof. Nikos E. Mastorakis. He is a Ph.D. holder in Computer Science and Engineering from Siksha 'O' Anusandhan, Bhubaneswar, and also an M.Tech in Computer Science from BIT Mesra. His research interests are Software Engineering, Artificial Intelligence, Machine Learning, and Data Mining