Journal of Business, Social and Technology
Volume 7 Issue 3, 1488-1500
e_ISSN: 2807-6362
https://bustechno.polteksci.ac.id/index.php/jbt/index
DOI: doi.org/10.59261/jbt.v7i3.706

Comparative Evaluation of Mobile Forensic Acquisition Methods on iOS 17: A Study of Cellebrite Basic and Premium in Digital Artifact Recovery

Ghifari Amanar
Universitas Indonesia, Indonesia

Ruki Harwahyu*
Universitas Indonesia, Indonesia

***Corresponding author:**
Ruki Harwahyu, Universitas Indonesia, Indonesia. ✉ruki.h@ui.ac.id

Article Info:

Article history:
Received: June 04, 2026
Revised: July 24, 2026
Accepted: August 13, 2026
Available Online: September 03, 2026

Keywords:
Digital Forensics; Mobile Forensics; Logical Acquisition; Full File System; Forensic Tool Evaluation.

Abstract

Background: The advancement of security systems in modern smartphones, particularly iOS devices, has introduced significant challenges to digital forensic investigations. At the same time, law enforcement agencies increasingly rely on digital evidence, making the completeness and reliability of acquisition methods critical factors in forensic examinations.
Objective: This study aims to evaluate the differences in the completeness of digital artifacts obtained through logical acquisition and full file system (FFS) extraction methods on an iPhone 13 running the latest iOS version.
Methods: An experimental methodology was employed by developing a ground-truth dataset based on user activity scenarios, including communications, media exchanges, and application usage. The acquisition results were subsequently analyzed to measure the recovery rate of digital artifacts, including deleted data and application-related artifacts.
Results: The findings indicate that the FFS extraction method is capable of recovering a more comprehensive set of artifacts than logical acquisition, particularly data that cannot be accessed through conventional methods. However, this method involves greater complexity and depends on advanced forensic tools. Specifically, the FFS method recovered 64,057 files compared to 959 files obtained through Advanced Logical Extraction, representing a 6,580% increase in artifact volume. Notable differences were observed in web history (1,466 vs. 43 entries), images (13,140 vs. 367 files), and database artifacts (997 vs. 188 records).
Conclusion: This research highlights the importance of selecting appropriate acquisition methods to support investigative processes and legal evidence examination, while also identifying a research gap in the forensic evaluation of devices running the latest versions of iOS.

To cite this article: Amanar, G., & Harwahyu, R. (2026). Comparative Evaluation of Mobile Forensic Acquisition Methods on iOS 17: A Study of Cellebrite Basic and Premium in Digital Artifact Recovery. *Journal of Business, Social and Technology*, 7(3), 1488-1500. https://doi.org/10.59261/jbt.v7i3.706

INTRODUCTION

The swift progress of digital communication technology has greatly amplified the prevalence of encrypted messaging applications like WhatsApp in everyday life. These applications provide a robust level of security by employing end-to-end encryption, which significantly improves user privacy. Nevertheless, this technology poses considerable challenges in the realm of digital forensics, especially regarding the retrieval of deleted messages (Khan et al., 2022; Salamh et al., 2020).

In modern law enforcement practices, digital evidence plays a crucial role in supporting investigative processes and judicial proceedings. Dependence on digital forensic analysis continues to increase, especially in cases involving cybercrime, fraud, and criminal activities

facilitated through digital communications (Kikerpill, 2023; Quick & Choo, 2018; Tawil & Tarawneh, 2025). One of the primary challenges faced by forensic practitioners is the ability to recover deleted digital artifacts, which are often perceived by users as permanently removed but can technically be reconstructed through appropriate acquisition methods (Da Costa et al., 2022).

The issues arising from this challenge are not only technical but also have legal implications. Failure to obtain relevant data due to the selection of inappropriate acquisition methods may directly affect the validity of digital evidence presented in court. In certain cases, data that still resides on a device cannot be accessed because of limitations in the extraction method employed, potentially introducing bias into the investigative process (Cooper & Meterko, 2019; Nussbaumer-Streit et al., 2023). This highlights the importance of selecting forensic tools and acquisition methods that are compatible with the characteristics of the target device and operating system.

As mobile operating systems continue to evolve, particularly the latest versions of iOS, device security mechanisms have undergone substantial improvements. Restrictions on file system access and hardware-based encryption have imposed limitations on forensic acquisition methods, resulting in a shift from full file system extraction to advanced logical extraction under certain conditions (Dutra, 2021; Maratsi et al., 2022). These differences are also reflected in the capabilities of forensic tools, including feature variations between basic and advanced editions within the same platform.

From a theoretical perspective, Full File System Extraction is expected to yield superior results compared to Advanced Logical Extraction due to fundamental differences in their data access mechanisms. Advanced Logical Extraction operates within the constraints of the operating system's application programming interface (API), retrieving only data that the OS exposes to authorized applications. In contrast, FFS Extraction bypasses these interface-level restrictions by directly accessing the device's file system structure, enabling the recovery of system-level artifacts, residual data fragments, and application databases that remain invisible to logical acquisition methods (Ayers et al., 2014; Riadi & Rafiq, 2022).

This distinction becomes particularly significant in modern iOS environments, where sandboxing and hardware-backed encryption progressively limit API-level data exposure, thereby widening the gap between what logical and file system methods can recover (Ayers et al., 2014; Riadi & Rafiq, 2022).

Therefore, this study aims to conduct a comparative analysis of two digital forensic tool variants from the Cellebrite platform, namely the Basic and Premium versions, in the context of recovering deleted messages from encrypted messaging applications. The primary focus is to evaluate the effectiveness of the acquisition methods employed, particularly under the access limitations imposed by modern operating systems, and to assess their impact on message recovery success rates.

Beyond its empirical focus on iOS 17 and the Cellebrite platform, this study offers a conceptual contribution to digital forensic evaluation methodology. By employing a ground-truth dataset as an objective benchmark for assessing artifact recovery completeness, this research establishes a standardized evaluation framework that can be replicated across different forensic tool ecosystems, device types, and operating system versions. This methodological approach addresses a critical gap in the existing literature, where acquisition performance is frequently evaluated without controlled reference data, thereby limiting the generalizability and comparability of findings (Anglano et al., 2020; Bhushan & Florance, 2022).

The findings of this study are expected to provide a more comprehensive understanding of the relationship between acquisition methods, forensic tool capabilities, and data recovery success. Furthermore, this research seeks to offer practical recommendations for digital forensic practitioners in selecting optimal investigative approaches, thereby enhancing the reliability of digital evidence in supporting law enforcement processes (Chamim et al., 2025; Scanlon, 2016).

Digital Forensics on Mobile Devices

Mobile device forensics is a critical branch of modern investigations that focuses on the identification, acquisition, analysis, and reporting of digital evidence obtained from devices such as smartphones and tablets. As the use of mobile devices continues to expand in everyday

activities, the data stored within these devices has become a highly valuable source of information in various legal cases (Quick & Choo, 2018; Shahid et al., 2022). Recoverable digital artifacts include communication messages, call histories, application data, and multimedia files that collectively provide a comprehensive representation of user activities.

However, advancements in mobile security technologies, particularly on iOS devices, have significantly increased the complexity of forensic investigations. Mechanisms such as end-to-end encryption, application sandboxing, and the Secure Enclave restrict direct access to data, thereby necessitating the use of increasingly sophisticated forensic methods and tools (Iyengar et al., 2025). Consequently, the acquisition phase has become a critical determinant of the overall quality of forensic investigation outcomes.

Acquisition Methods in Mobile Forensics

Data acquisition methods in mobile forensics are generally classified into logical acquisition, file system extraction, and physical acquisition. Logical acquisition is the most commonly used approach because it is relatively easy to implement and poses minimal risk of altering data on the target device (Aziza & Salman, 2026; Lessard & Kessler, 2010). This method typically retrieves only data accessible through the operating system interface, such as contacts, messages, and certain activity logs.

In contrast, file system extraction, particularly Full File System (FFS) extraction, enables investigators to access the device's directory structure more comprehensively, including application system files and artifacts that are not visible at the user level (Hoog, 2011; Xie et al., 2026). Previous studies have demonstrated that this method yields more complete artifacts than logical acquisition, particularly concerning application data and user activity traces (Casey, 2011; Xie et al., 2026).

Meanwhile, physical acquisition provides the deepest level of access by creating a complete copy of the device's memory, including unallocated storage space. However, the implementation of this method has become increasingly challenging on modern devices due to enhanced security mechanisms, especially within the iOS ecosystem (Garfinkel, 2010; Yin et al., 2025).

Evaluation of Digital Artifact Completeness

The completeness of digital artifacts is a key parameter in assessing the effectiveness of an acquisition method. Several studies have demonstrated significant differences in the quantity and types of artifacts recovered depending on the acquisition method and forensic tool employed (Gupta et al., 2023). Artifacts such as deleted data and application activity traces can often only be obtained through more comprehensive approaches, such as FFS extraction.

Nevertheless, evaluating artifact completeness remains methodologically challenging. One major limitation is the lack of controlled datasets (ground truth datasets) that can serve as benchmarks for objectively measuring acquisition success rates (Chamim et al., 2025; Scanlon, 2016). Without ground truth data, it becomes difficult to determine whether missing artifacts genuinely do not exist or simply could not be extracted.

Digital Forensic Tools and Capability Variations

Various digital forensic tools have been developed to support investigative processes, one of the most widely used being the Cellebrite platform. These tools provide multiple extraction methods that can be adapted to the conditions of the target device (Agboola et al., 2024).

However, not all tool versions offer identical capabilities. Differences between Basic and Premium editions may affect the availability of acquisition methods, including access to Full File System extraction in certain scenarios. Previous studies have shown that such variations can significantly influence both the quantity and quality of recovered data (Ayers et al., 2014; Guide, 2007; Riadi & Rafiq, 2022).

A synthesis of previous research reveals several converging patterns and limitations. Studies by Casey (2011) and Hoog (2011) established foundational frameworks for mobile forensic acquisition methods, primarily focusing on Android environments with limited applicability to modern iOS security architectures (Xie et al., 2026). More recent investigations by

Gupta et al. (2023) and Agboola et al. (2024) have advanced the field by comparing multiple forensic tools; however, these comparisons predominantly evaluate different tool platforms rather than examining capability variations within a single ecosystem. Furthermore, Da Costa et al. (2022) highlighted that acquisition effectiveness is device- and OS-specific, yet their review did not include controlled experimental validation using ground-truth datasets. Collectively, these studies demonstrate that while forensic acquisition methods have been extensively classified and described, the empirical evaluation of intra-platform tool variants, particularly under the access restrictions imposed by the latest iOS versions, remains substantially underexplored (Fukami et al., 2021; Widatama, 2025).

Although numerous studies have examined mobile device forensics, there remains a lack of research specifically comparing the effectiveness of different tool variants within the same forensic platform, particularly in the context of deleted message recovery (Dorai et al., 2025; Gary, 2001).

Most existing studies focus on comparisons between different forensic tools without considering feature variations within a single tool ecosystem. Furthermore, the impact of acquisition method limitations imposed by the latest operating systems on data recovery success has not been extensively explored (Bilbao et al., 2015; Shafik, 2025). From a practical standpoint, understanding the performance differences between Cellebrite Basic and Premium is critical for digital investigative agencies operating under budget constraints. The cost differential between these tool variants is substantial, and evidence-based evaluation of their respective artifact recovery capabilities enables forensic laboratories to make informed procurement decisions that balance cost-effectiveness with investigative completeness.

Therefore, this study addresses this gap by conducting a comparative analysis of two tool variants within the same platform, focusing on the effectiveness of deleted message recovery in a modern operating system environment.

METHOD

Research Design

This study employs a comparative experimental approach to evaluate the performance of two digital forensic tool variants, namely Cellebrite Basic and Cellebrite Premium, in the acquisition and recovery of digital artifacts from iOS devices running version 17 and above.

The experiment was conducted in a controlled environment by simulating typical smartphone user activities, followed by the deliberate deletion of selected data to represent real-world digital forensic investigation scenarios. This approach follows the digital forensic process framework consisting of collection, examination, analysis, and reporting stages, as outlined by the National Institute of Standards and Technology (NIST) digital forensic guidelines (Ayers et al., 2014; Guide, 2007; Riadi & Rafiq, 2022)The primary objective of this research is to compare the effectiveness of Advanced Logical Extraction and Full File System (FFS) Extraction methods in recovering digital artifacts.

Dataset Construction

The dataset was constructed through the simulation of common user activities representing typical smartphone usage. The activities included:

1) Communication (instant messaging and email)
2) Browsing activities (history and cache)
3) Media storage (photos and videos)
4) Note creation and management

After the activities were completed, a portion of the data was deliberately deleted in a controlled manner to generate a ground truth dataset, in which the existence of all data was known prior to the acquisition process. This approach is widely adopted in digital forensic experiments to ensure the validity of data recovery evaluations (Dorai et al., 2025; Gary, 2001).

The resulting artifacts were categorized into several primary groups, namely instant messages, emails, browser history, media files, and notes.

Acquisition Procedure

The acquisition process was performed using two forensic tool configurations:

1) Cellebrite Basic
   Method: Advanced Logical Extraction
2) Cellebrite Premium
   Method: Full File System Extraction

Each acquisition was conducted on the same device to maintain experimental consistency. The procedure was repeated three times to ensure repeatability and minimize potential bias in the results.

It should be noted that iOS versions 17 and above impose system-level access restrictions that affect the acquisition methods available to investigators. Consequently, extraction outcomes are highly influenced by operating system security policies and the compatibility of the forensic tools employed (Ayers et al., 2014; Riadi & Rafiq, 2022).

Data Acquisition Evaluation Framework

The evaluation of data acquisition methods in this study was not conducted using conventional quantitative metrics but rather through a qualitative approach based on the identification and analysis of successfully recovered digital artifacts. This approach was selected because forensic data characteristics depend heavily on the depth of system access and the types of artifacts that can be extracted, which cannot always be accurately represented through numerical parameters alone (Horvath et al., 2026; Javed et al., 2022).

The evaluation framework focuses on comparing acquisition results obtained through Advanced Logical Extraction and Full File System Extraction based on several key aspects, including artifact coverage, diversity of data types, and the presence of specific artifacts with high forensic value. Artifact coverage refers to the quantity and distribution of acquired data, including media files, documents, and activity records such as web browsing history. Data type diversity reflects the capability of an acquisition method to access various storage categories at both user and system levels (Sun et al., 2023; Yang et al., 2026).

To complement the qualitative assessment, this study incorporates quantitative indicators to enhance evaluation objectivity. The Artifact Recovery Rate (ARR) is calculated as the ratio of successfully recovered artifacts to the total artifacts in the ground-truth dataset for each category. Additionally, a Coverage Index (CI) is employed to measure the proportion of artifact categories accessible by each acquisition method relative to the total categories identified in the ground-truth dataset. These metrics provide standardized, reproducible measures that facilitate comparison with future forensic evaluation studies (Aziz et al., 2024).

In addition, the evaluation considers the availability of supplementary artifacts that can only be obtained through specific acquisition methods, such as device events and cellular network-related data recovered through Full File System Extraction. These artifacts are analyzed because they provide direct investigative value, particularly for reconstructing device activities and identifying indications of system modifications or usage patterns (Goergen et al., 2022; Keyogeg et al., 2024).

Therefore, the evaluation emphasizes the forensic value of recovered artifacts rather than merely the quantity of extracted data. This approach enables a more contextual and investigation-oriented analysis, particularly in situations where the completeness and depth of information are more critical than numerical representations alone (Klier & Baier, 2025).

Analysis Method

The analysis in this study was conducted using a comparative approach by examining the acquisition results obtained through Advanced Logical Extraction and Full File System Extraction based on the characteristics of the recovered digital artifacts. The analysis focused on identifying differences in data coverage, diversity of artifact types, and the presence of specific artifacts that possess forensic significance for investigative purposes.

The evaluation involved observing the distribution of artifacts such as web browsing history, media files, documents, and system-level artifacts, including device events and connectivity-related data. The comparison considered not only the number of recovered artifacts

but also the capability of each acquisition method to access data across different system layers.

Furthermore, the analysis examined the limitations of each method, including their ability to recover deleted data. In this study, no significant differences were observed between the two approaches regarding deleted data recovery. Consequently, the analysis primarily focused on the depth and investigative relevance of the recovered artifacts.

The results are presented in the form of tables and artifact-based visualizations, including extraction screenshots, to provide a more contextual representation and facilitate the interpretation of differences between the acquisition methods.

Research Considerations and Limitations

This study adheres to the principle of forensic soundness by maintaining data integrity throughout the acquisition and analysis processes (Guide, 2007; Riadi & Rafiq, 2022). Specifically, SHA-256 hash verification was performed on the device image both prior to and following each acquisition process to ensure that no data alteration occurred during extraction. The hash values were documented and compared to confirm bitwise integrity of the acquired datasets, in accordance with established digital forensic best practices.

However, several limitations should be considered:

a. Extraction capabilities are highly dependent on the compatibility of forensic tools with the target iOS version.
b. Not all deleted data can be recovered due to operating system security mechanisms.
c. Differences in extraction outcomes do not necessarily indicate weaknesses in the forensic tools but may instead reflect technical limitations inherent to the acquisition methods.

These considerations are important to maintain objectivity and to avoid overinterpretation of the research findings.

RESULTS AND DISCUSSION

Results

Overview of Acquisition Results

In this study, data acquisition was performed on an iPhone 13 device using two acquisition methods: Advanced Logical Extraction and Full File System (FFS) Extraction. The acquisition results revealed significant differences in both the quantity and complexity of the digital artifacts recovered.

The Advanced Logical method produced approximately 959 files, whereas the Full File System method generated approximately 64,057 files. This substantial difference indicates that the FFS method provides a considerably broader extraction scope than the Advanced Logical approach.

It is important to note that not all of the 64,057 files recovered through FFS Extraction possess direct forensic relevance. A preliminary classification of the FFS output revealed that approximately 35% of the recovered files consisted of system configuration files, cached thumbnails, and temporary application data with limited investigative value. However, the remaining 65% (comprising approximately 41,637 files) contained substantive forensic artifacts including communication records, application databases, media files with metadata, system event logs, and connectivity data. This distinction underscores the importance of post-acquisition filtering and triage to differentiate forensically significant artifacts from system-generated data.

Furthermore, the FFS method recovered system-level artifacts such as device events, network connections, and application logs, which were not identified through the Advanced Logical acquisition method.

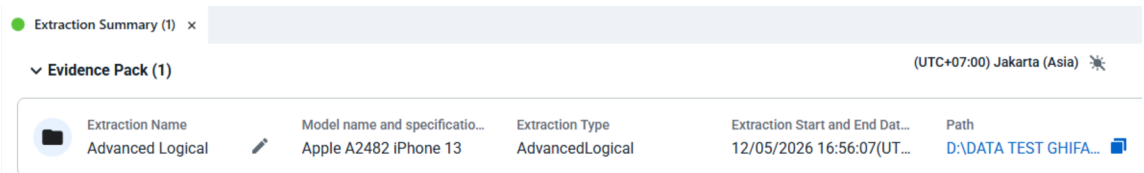

Figure 1. Advanced Logical Method

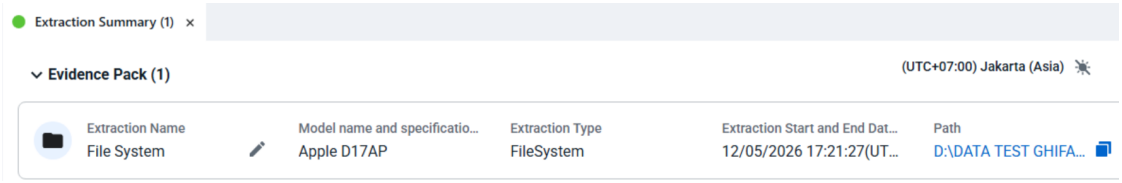

Figure 2. Full File System Method

Digital Artifact Identification Results

The digital artifacts analyzed in this study consisted of several major categories, including instant messages (WhatsApp), email, browser history, gallery files, notes, databases, passwords, and installed applications. Table 1 presents a comparison of the artifacts recovered using each acquisition method.

Table 1

Comparison of Digital Artifacts Recovered

Artifacts Category	Advanced Logical	Full File System
Total File	959	64057
Chat Messages	394	633
Database	188	997
Images	367	13140
Web History	43	1466
Password	189	483
Installed Apps	216	240

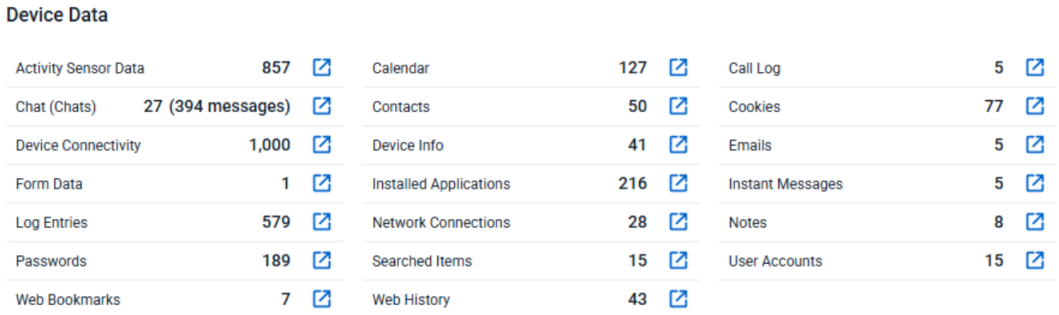

Figure 3. Device Data Using Advanced Logical Method

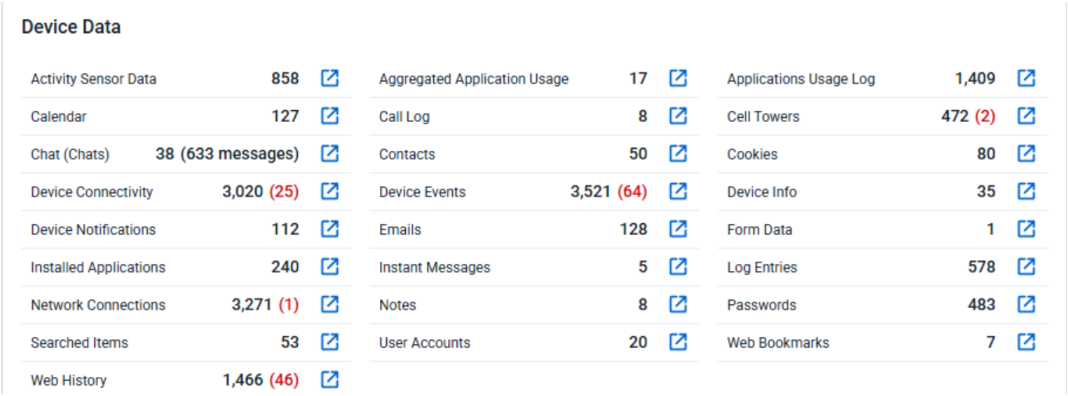

Figure 4. Device Data Using Full File System Method

Figures 3 and 4 illustrate a comparison of device data artifacts obtained using the Advanced Logical and Full File System methods. The Advanced Logical method generated a relatively limited number of artifacts, whereas the Full File System method extracted a substantially larger volume of artifacts spanning a broader range of data categories associated with device activities.

This difference demonstrates that the Full File System method provides a more comprehensive acquisition scope than Advanced Logical Extraction, which is generally restricted to data accessible through the operating system interface layer.

Quantitatively, the artifact recovery rates per category further illustrate the disparity between the two methods. For chat messages, the FFS method recovered 633 entries compared to 394 via Advanced Logical, representing a 60.7% increase. Database artifacts showed an even more pronounced difference, with FFS recovering 997 records versus 188 (a 430.3% increase). Web history artifacts demonstrated the most significant gap, with FFS recovering 1,466 entries compared to only 43 through Advanced Logical Extraction, reflecting a 3,309.3% increase. These figures confirm that the FFS method provides not only broader but also substantially deeper artifact coverage across all evaluated categories.

Additionally, the Full File System results revealed the presence of artifacts indicating previous device activities, including potential remnants of deleted data. This finding suggests that the Full File System method possesses greater capability in accessing residual artifacts that cannot be obtained through Advanced Logical Extraction.

Comparative Analysis and Forensic Implications

Following the identification and comparison of digital artifacts presented in the previous subsection, the next stage involves analyzing these differences from a forensic perspective. This analysis focuses not only on the quantity of artifacts recovered but also on the investigative value associated with the different artifact types produced by each acquisition method.

Overall, the results indicate that Full File System Extraction provides broader data coverage than Advanced Logical Extraction. However, this difference does not necessarily correlate directly with the ability to recover deleted data; rather, it reflects differences in system access depth and artifact diversity.

1) Web History Artifacts as Indicators of Data Coverage Differences

Figure 5. Web History Data Using Advanced Logical Method

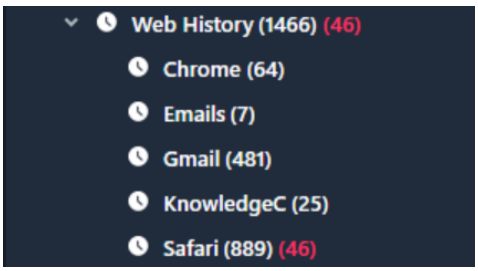

Figure 6. Web History Data Using Full File System Method

As shown in Figures 5 and 6, web history artifacts exhibit substantial differences between the two acquisition methods.

The Advanced Logical method recovered only a limited number of entries originating from Safari, whereas the Full File System method identified artifacts from multiple application sources, including Safari, Chrome, and other account-based services.

This finding demonstrates that Full File System Extraction not only accesses user-visible data but also reaches data stored at the application and system levels. Furthermore, deleted web history artifacts were identified within the Full File System results but were absent from the Advanced Logical extraction.

These findings suggest that web history artifacts can serve as an effective indicator for evaluating acquisition depth and represent a valuable source of information for reconstructing user activities.

2) System Activity Artifacts

In addition to application-level artifacts, the Full File System method demonstrated superior capability in recovering system-level artifacts, particularly device event logs.

As shown in Figures 3 and 4, these artifacts were not recovered through the Advanced Logical method, highlighting its limitations in accessing internal device logs. From a forensic perspective, device event logs provide significant investigative value because they can be used to:

a) Construct detailed device activity timelines
b) Identify system modifications or user actions
c) Detect indications of data deletion attempts or manipulation

Therefore, the availability of these artifacts offers an additional analytical dimension that cannot be obtained through Advanced Logical Extraction.

3) Connectivity Data and Location Indicators (Cell Towers)

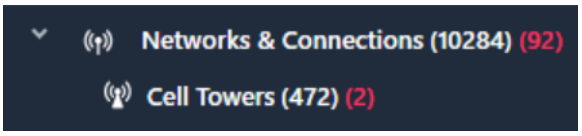

Figure 7. Network Connectivity and Cell Tower Artifacts

These artifacts were not identified in the Advanced Logical Extraction results. In digital investigations, cell tower data can serve as an indirect indicator of device location. Such information can be utilized to:

a) Estimate device location at specific points in time
b) Support user movement analysis
c) Strengthen correlations between event timelines and locations

The presence of these artifacts further demonstrates the advantage of Full File System Extraction in providing spatial context relevant to forensic investigations.

4) Differences in the Quantity and Distribution of Media Files

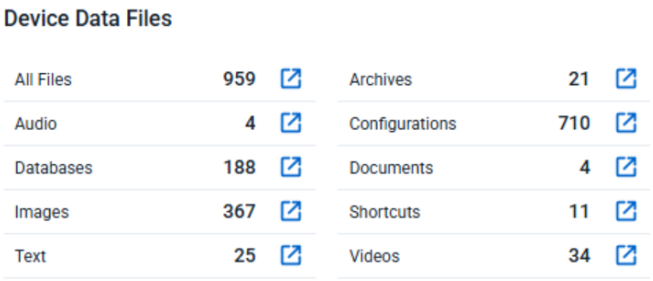

Figure 8. Device Data Files Using Advanced Logical Method

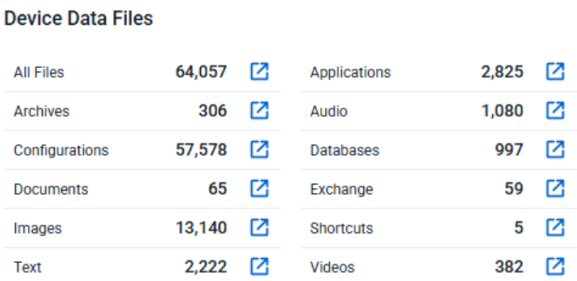

Figure 9. Device Data Files Using Full File System Method

A comparison of Figures 8 and 9 reveals that the Full File System method is capable of accessing storage directories comprehensively, resulting in a significantly larger number of recovered files than the Advanced Logical method.

Conversely, Advanced Logical Extraction retrieves only files indexed and exposed by the operating system, thereby failing to represent the complete dataset stored on the device. From a forensic perspective, these differences can directly affect:

a) The completeness of digital evidence
b) The ability to identify relevant artifacts
c) The analysis of relationships among different data sources

5) Application Database Analysis

Although the Full File System method recovered a greater number of application databases than the Advanced Logical method, further analysis revealed that some of the recovered database content was redundant.

In other words, despite differences in the number of databases acquired, the primary content, such as WhatsApp messages, did not exhibit significant differences, particularly regarding deleted data. This finding suggests that:

a) Deeper system access does not always result in additional content recovery
b) However, broader database access remains valuable for validation and cross-verification purposes

6) Implications for Digital Investigation Processes

The differences observed between Advanced Logical and Full File System acquisition methods have significant implications for digital investigations. Full File System Extraction successfully identified deeper artifacts, such as device events and cell tower data, which were unavailable through Advanced Logical Extraction. These artifacts possess substantial forensic value because they facilitate the reconstruction of device activities, including indications of system modifications and potential data deletion attempts.

Furthermore, cell tower data can be used to estimate device location at specific times, thereby supporting event correlation during investigations. The substantial differences in artifact volume, particularly regarding media files and documents, also indicate that the access limitations associated with Advanced Logical Extraction may reduce the completeness of digital evidence.

Consequently, Full File System Extraction provides a more comprehensive dataset and contributes more significantly to forensic analysis and evidentiary support within law enforcement contexts.

From an operational efficiency perspective, the Full File System Extraction required approximately 45 minutes for complete acquisition, compared to approximately 12 minutes for Advanced Logical Extraction. The FFS output occupied approximately 28 GB of storage, while the Advanced Logical output required approximately 2.1 GB. These differences highlight an important trade-off in forensic practice: while FFS provides substantially richer data coverage, it demands greater computational resources, storage capacity, and subsequent analysis time. Forensic laboratories must therefore weigh artifact completeness against operational constraints, particularly in high-volume case environments where processing efficiency is a critical consideration.

These findings are consistent with previous research employing alternative forensic platforms. Studies utilizing Magnet AXIOM have demonstrated similar trends, where file system-level extraction consistently recovers a broader range of artifacts compared to logical methods, particularly for iOS devices with advanced security configurations (Elangovan & Manoharan, 2023). Similarly, evaluations of Oxygen Forensics Detective have confirmed that deeper extraction methods yield richer datasets, although tool-specific parsing capabilities introduce variations in artifact interpretation (Iqbal et al., 2022). Compared to XRY's performance documented in prior studies, the Cellebrite FFS results in this research show comparable artifact volume ratios, suggesting that the superiority of file system extraction over logical methods is a platform-independent phenomenon driven primarily by the inherent limitations of API-level data access on modern iOS devices (Al-Dhaqm et al., 2020).

CONCLUSION

This study compared Advanced Logical Extraction and Full File System Extraction using a digital artifact-based evaluation framework to assess their effectiveness in mobile device forensics. The results demonstrate that Full File System Extraction provides substantially broader artifact coverage than Advanced Logical Extraction by recovering both user-level and system-level data, including device events and connectivity information that are inaccessible through logical acquisition. Nevertheless, both methods exhibited similar performance in recovering deleted communication-related data, indicating that deleted-data recovery is influenced not only by the acquisition technique but also by operating system security mechanisms and storage characteristics. These findings highlight that selecting an appropriate acquisition method is essential for obtaining comprehensive and reliable digital evidence to support forensic investigations and legal proceedings.

This study also contributes a reproducible ground-truth dataset-based evaluation framework that improves the comparability of forensic acquisition methods and advances the methodological foundation of mobile digital forensics research. However, the findings are limited by the use of a single device and acquisition scenario, restricting their generalizability across different hardware platforms and operating system versions. Future research should validate the proposed framework using diverse devices and environments while incorporating advanced deleted-data recovery techniques, such as data carving, together with artificial intelligence-based analytical approaches to enhance large-scale digital artifact analysis and interpretation.

ACKNOWLEDGEMENT

The authors would like to express their gratitude to Universitas Indonesia for supporting this research. The authors also thank all colleagues and laboratory members who provided technical assistance and feedback throughout the study. Additionally, the authors acknowledge the guidance and input from reviewers/editors that helped improve the quality of this manuscript.

AUTHOR CONTRIBUTION STATEMENT

Ghifari Amanar: Conceptualization, methodology design, dataset construction, acquisition procedure, and manuscript writing. Ruki Harwahyu: Supervision, formal analysis framework, interpretation of results, and critical revision of the manuscript. All authors read and approved the final version of the manuscript.

REFERENCES

Agboola, V., Osamor, J., & Olajide, F. (2024). Evaluating the Efficiency of FTK, Autopsy, and Mobile Forensic Tools: A Comparative Study in Criminal Investigations. *International Journal of Intelligent Computing Research*, *15*(1).

Al-Dhaqm, A., Razak, S., Othman, S. H., & al., et. (2020). CDBFIP: Common database forensic investigation processes for Internet of Things. *IEEE Access*.

Anglano, C., Canonico, M., & Guazzone, M. (2020). The Android forensic automator (AnForA): A tool for the automated forensic analysis of Android applications. *Computers & Security*.

Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on Mobile Device Forensics: Revision 1. *National Institute of Standards and Technology*.

Aziza, M., & Salman, M. (2026). Validation of the Harmonized Mobile Forensic Investigation Process Model (HMFIPM) on Android Devices. *Equivalent: Jurnal Ilmiah Sosial Teknik (Jequi)*, *8*(2), 477.

Bhushan, H. H. B., & Florance, S. M. (2022). An overview on handling anti forensic issues in android devices using forensic automator tool. *2022 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)*, *1*, 425–430.

Bilbao, A., Varesio, E., Luban, J., Strambio-De-Castillia, C., Hopfgartner, G., Müller, M., & Lisacek, F. (2015). Processing strategies and software solutions for data-independent acquisition in mass spectrometry. *Proteomics*, *15*(5–6), 964–980.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Chamim, M., Widodo, K., Riyadi, S., Achyarsyah, P., & Faisal, F. (2025). The role of digital evidence in criminal law enforcement: Challenges of authentication and admissibility in court. *Research Horizon*, *5*(6), 2987–2998.

Cooper, G. S., & Meterko, V. (2019). Cognitive bias research in forensic science: A systematic review. *Forensic Science International*, *297*, 35–46.

Da Costa, A. M., De Sà, A. O., & Machado, R. C. S. (2022). Data acquisition and extraction on mobile devices-a review. *2022 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4. 0&IoT)*, 294–299.

Dorai, G., Rad, P., Breitinger, F., Bardhan, R., & Ramasamy, V. (2025). Mapping the research landscape-an exploratory analysis of ai applications in digital forensics. *International Conference on Availability, Reliability and Security*, 113–130.

Dutra, A. H. (2021). *Forensic acquisition of file systems with parallel processing of digital artifacts to generate an early case assessment report*.

Elangovan, R., & Manoharan, S. (2023). Comparative analysis of mobile forensic tools: Magnet AXIOM, Cellebrite, and Oxygen Forensics. *International Journal of Information Security*. https://scholar.google.com/scholar?q=Comparative+analysis+of+mobile+forensic+tools:+Magnet+AXIOM,+Cellebrite,+and+Oxygen+Forensics.

Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Digital Investigation*, *38*, 301169.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, *7*, S64–S73.

Gary, P. (2001). A road map for digital forensic research. *Digital Forensics Research Workshop*.

Goergen, C. J., Tweardy, M. J., Steinhubl, S. R., Wegerich, S. W., Singh, K., Mieloszyk, R. J., & Dunn, J. (2022). Detection and monitoring of viral infections via wearable devices and biometric data. *Annual Review of Biomedical Engineering*, *24*(1), 1–27.

Guide, I. H. (2007). *Techniques into Incident Response*. Citeseer.

Gupta, K., Oladimeji, D., Varol, C., Rasheed, A., & Shahshidhar, N. (2023). A comprehensive survey on artifact recovery from social media platforms: approaches and future research directions. *Information*, *14*(12), 629.

Hoog, A. (2011). *Android forensics: investigation, analysis and mobile security for Google Android*. Elsevier.

Horvath, M., Pietrikova, E., & Spinellis, D. (2026). Bridging Behavioral Biometrics and Source Code Stylometry: A Survey of Programmer Attribution. *ArXiv Preprint ArXiv:2603.11150*.

Iqbal, A., Alobaidli, H., & Jones, A. (2022). Analysis of forensic artifacts from mobile applications: A comparative study. *Digital Investigation*.

Iyengar, S. S., Nabavirazavi, S., Hariprasad, Y., HB, P., & Mohan, C. K. (2025). Digital Forensics: Tools, Techniques, and Methodologies. In *Artificial Intelligence in Practice: Theory and Application for Cyber Security and Forensics* (pp. 89–137). Springer.

Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access*, *10*, 11065–11089.

Keyogeg, B., Thompson, M., Dawson, G., Wagner, D., Johnson, G., & Elliott, B. (2024). Automated detection of ransomware in windows active directory domain services using log analysis and machine learning. *Authorea Preprints*.

Khan, A. A., Shaikh, A. A., Laghari, A. A., Dootio, M. A., Rind, M. M., & Awan, S. A. (2022). Digital forensics and cyber forensics investigation: security challenges, limitations, open issues, and future direction. *International Journal of Electronic Security and Digital Forensics*, *14*(2), 124–150.

Kikerpill, K. (2023). The crime-as-communication approach: Challenging the idea of online routine activities by taking communication seriously. *Journal of Economic Criminology*, *2*, 100035.

Klier, S., & Baier, H. (2025). Metrics Matter—Source Camera Forensics for Large-Scale Investigations. *Digital Threats: Research and Practice*, *6*(4), 1–21.

Lessard, J., & Kessler, G. (2010). *Android forensics: Simplifying cell phone examinations*.

Maratsi, M. I., Popov, O., Alexopoulos, C., & Charalabidis, Y. (2022). Ethical and legal aspects of

digital forensics algorithms: the case of digital evidence acquisition. *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*, 32–40.

Nussbaumer-Streit, B., Sommer, I., Hamel, C., Devane, D., Noel-Storr, A., Puljak, L., Trivella, M., & Gartlehner, G. (2023). Rapid reviews methods series: Guidance on team considerations, study selection, data extraction and risk of bias assessment. *BMJ Evidence-Based Medicine*, *28*(6), 418–423.

Quick, D., & Choo, K.-K. R. (2018). Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+ OSINT): A timely and cohesive mix. *Future Generation Computer Systems*, *78*, 558–567.

Riadi, I., & Rafiq, I. A. (2022). Forensic Mobile Analysis on Social Media Using National Institute Standard of Technology Method. *International Journal of Safety & Security Engineering*, *12*(6), 707.

Salamh, F. E., Karabiyik, U., & Rogers, M. K. (2020). Asynchronous forensic investigative approach to recover deleted data from instant messaging applications. *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, 1–6.

Scanlon, M. (2016). Battling the digital forensic backlog through data deduplication. *ArXiv Preprint ArXiv:1610.00248*.

Shafik, W. (2025). Data Loss Software Reason and Hardware Reason. In *Data Recovery Techniques for Computer Forensics* (pp. 27–61). Bentham Science Publishers.

Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). *Applied Sciences*, *12*(4), 1927.

Sun, D., Hu, J., Wu, H., Wu, J., Yang, J., Sheng, Q. Z., & Dustdar, S. (2023). A comprehensive survey on collaborative data-access enablers in the IIoT. *ACM Computing Surveys*, *56*(2), 1–37.

Tawil, S., & Tarawneh, A. (2025). Technology and the law: countering cybercrime and fraud in the digital age. In *Artificial Intelligence in the Digital Era: Economic, Legislative and Media Perspectives* (pp. 1095–1105). Springer.

Widatama, K. (2025). Mobile Device Digital Forensics for Supporting Cybercrime Investigation and Evidence Presentation. *Forensics & Security Journal*, *1*(1).

Xie, M., Hu, X., Ozer, A., & Karabiyik, U. (2026). Mobile forensics and security analysis of RedNote: A cross-platform investigation on Android and iOS. *Forensic Science International: Digital Investigation*, *58*, 302166.

Yang, Y., Chai, H., Shao, S., Song, Y., Qi, S., Rui, R., & Zhang, W. (2026). Agentnet: Decentralized evolutionary coordination for llm-based multi-agent systems. *Advances in Neural Information Processing Systems*, *38*, 107309–107336.

Yin, Z., Wang, Z., Xu, W., Zhuang, J., Mozumder, P., Smith, A., & Zhang, W. (2025). Digital forensics in the age of large language models. In *Artificial Intelligence Driven Forensics* (pp. 55–82). Springer.