Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Forensic Artefact Recovery and Evidence Preservation in Cloud-Based Messaging Applications

Patricia Ghann

patricia.ghann@ktu.edu.gh

Koforidua Technical University https://orcid.org/0000-0003-3072-2795

Research Article

Keywords: Cloud forensics, Mobile forensics, Messaging applications, Digital evidence, End-to-end encryption, Evidence preservation

Posted Date: May 19th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9741742/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

Abstract

Cloud-based messaging applications such as WhatsApp, Telegram, Signal, and iMessage increasingly depend on distributed cloud infrastructures, synchronization services, and remote storage mechanisms to support seamless communication across multiple devices. While these architectures enhance usability and accessibility, they introduce significant challenges for digital forensic investigations because evidentiary artefacts are distributed across devices, cloud services, and network environments. Traditional device-centric forensic approaches are therefore insufficient for comprehensive evidence acquisition.

This study investigates the recovery and preservation of forensic artefacts from cloud-based messaging applications across Android, iOS, and associated cloud infrastructures. Using controlled experimental environments, the research evaluates logical device acquisition, cloud-based acquisition, API analysis, and network artefact examination under conditions involving encryption, cloud synchronization, and ephemeral messaging.

The findings demonstrate that although message content is increasingly protected by end-to-end encryption, valuable metadata, synchronization records, authentication artefacts, and residual traces remain recoverable across multiple forensic layers. The study further proposes a structured multi-layer forensic framework that integrates device-level, cloud-level, and network-level acquisition while preserving evidential integrity and chain of custody.

The results indicate that combining cloud-aware acquisition techniques significantly improves evidential completeness, reliability, and legal admissibility in modern cloud-centric messaging investigations.

1. Introduction

Cloud computing has fundamentally transformed the architecture of modern messaging applications. Platforms such as WhatsApp Cloud Backup, Telegram, Signal, and Apple iMessage increasingly store user data across distributed cloud infrastructures rather than solely on local devices. Messages, attachments, metadata, and backups may be synchronized across multiple endpoints, enabling seamless user access but complicating forensic investigations. Cloud-based messaging applications distribute evidentiary artefacts across multiple layers, as illustrated in Fig. 1.

Digital forensic investigators traditionally rely on device-centric acquisition techniques to recover artefacts from mobile phones. However, the migration of messaging data to cloud environments renders these techniques incomplete, as critical evidence may be fragmented across devices, cloud servers, and network communications. The widespread adoption of end-to-end encryption (E2EE), ephemeral messaging, and encrypted cloud backups further exacerbates these challenges by restricting direct access to content while preserving only limited metadata.

Recent research highlights the growing need for cloud-aware forensic methodologies capable of acquiring evidence from distributed and encrypted messaging ecosystems. Investigators must now consider cloud credentials, synchronization logs, API responses, and residual network artefacts in addition to traditional device artefacts. Failure to do so risks evidence loss, incomplete reconstruction of events, and challenges to legal admissibility.

This study addresses these challenges by systematically examining forensic artefact recovery from cloud-based messaging applications. Through controlled experimentation, the research evaluates which acquisition techniques yield the most reliable and court-admissible evidence. The work further proposes a forensic framework that integrates device-level, cloud-level, and network-level evidence acquisition while maintaining evidential integrity.

Research Problem

Traditional mobile forensic techniques primarily focus on local device acquisition and are increasingly ineffective in cloud-centric messaging environments where evidentiary artefacts are distributed across cloud services, synchronized devices, and encrypted communication channels. The growing adoption of end-to-end encryption and ephemeral messaging further complicates evidence recovery and preservation.

Research Aim

This study aims to investigate forensic artefact recovery and evidence preservation techniques in cloud-based messaging applications.

Research Objectives

1. To identify recoverable forensic artefacts across distributed acquisition layers.
2. To evaluate the effectiveness of cloud-aware forensic acquisition techniques.
3. To assess evidential reliability and legal admissibility.
4. To propose an integrated forensic framework suitable for cloud-centric messaging investigations.

2. Research Contributions

This paper makes the following contributions to the field of digital and cloud forensics:

1. A systematic analysis of recoverable forensic artefacts from cloud-based messaging applications across Android, iOS, and cloud services.
2. An evaluation of logical, cloud, API-based, and network acquisition techniques in the presence of encryption and cross-device synchronization.

3. Identification of evidentiary limitations introduced by end-to-end encryption and ephemeral messaging features.
4. Development of a structured forensic framework for cloud-based messaging investigations that preserves chain of custody and legal admissibility.
5. Practical guidance for investigators on evidence acquisition strategies in cloud-centric communication environments.

2. Related Work

The rapid adoption of cloud-based messaging applications has significantly altered the landscape of digital forensic investigations[1–4]. Traditional mobile forensic methodologies, which focus primarily on local device storage, are increasingly insufficient in environments where user data is distributed across cloud infrastructures, synchronized across devices, and protected by strong encryption mechanisms[5, 2]. As a result, a growing body of research has examined the forensic challenges and opportunities associated with cloud computing, mobile messaging applications, and evidence preservation.

2.1 Mobile Forensics and Messaging Applications

Early studies in mobile forensics concentrated on artefact recovery from local device storage, including application databases, file systems, and volatile memory [6, 7]. Researchers demonstrated that messaging applications such as SMS, MMS, and early instant messaging platforms stored recoverable artefacts in plaintext databases or structured files on mobile devices [8, 9]. These artefacts included message content, timestamps, contact identifiers, and media attachments, which could be extracted using logical or physical acquisition techniques. The use of both commercial and open-source forensic tools for mobile and cloud investigations is consistent with established digital forensic practice[10–12]

However, the evolution of modern messaging applications has introduced advanced security mechanisms, including sandboxed storage, encrypted databases, and secure key management. Studies examining applications such as WhatsApp and Telegram have shown that while some artefacts remain accessible on devices, critical information may be encrypted or partially removed following user actions such as deletion, logout, or application updates. This has prompted researchers to emphasize the importance of correlating artefacts across multiple sources rather than relying solely on device-level acquisition.

2.2 Cloud Forensics and Distributed Evidence

Cloud forensics has emerged as a specialized subdomain of digital forensics, addressing the challenges of acquiring and preserving evidence stored in remote, virtualized, and distributed environments[1, 2, 13]. Unlike traditional digital forensics, cloud forensics must contend with multi-tenancy, jurisdictional issues, limited investigator control, and dependency on service providers.

Prior research has identified cloud artefacts such as synchronization logs, backup records, authentication tokens, and access metadata as valuable sources of evidence [14, 15]. Studies demonstrate that even when message content is encrypted, metadata retained in cloud services can provide critical investigative insights, including communication patterns, account usage timelines, and device associations[16, 17]. Nevertheless, the volatility of cloud data and provider-specific architectures complicates standardized forensic acquisition. However, many existing studies focus primarily on isolated cloud acquisition techniques without sufficiently addressing the interdependence between device-level and cloud-level artefacts in real-world investigations.

2.3 End-to-End Encryption and Ephemeral Messaging

The widespread deployment of end-to-end encryption (E2EE) has significantly strengthened user privacy but simultaneously constrained forensic access. Applications such as Signal and WhatsApp employ E2EE to ensure that message content is accessible only to communicating parties, rendering server-side content acquisition ineffective.

Several researchers have examined the forensic implications of E2EE and ephemeral messaging features, such as self-destructing messages and disappearing chats[18]. Findings indicate that while message content may be unrecoverable after deletion, residual artefacts, including message identifiers, timestamps, key exchange metadata, and notification remnants, may persist on devices or within system logs. These artefacts, although indirect, can still contribute to evidentiary reconstruction when analyzed holistically. Although end-to-end encryption strengthens privacy protection, existing research often underestimates the evidential value of residual metadata and synchronization artefacts that persist beyond message deletion.

2.4 API and Network-Based Evidence Acquisition

As direct access to message content becomes increasingly restricted, forensic research has expanded toward application programming interface (API) analysis and network traffic examination. Studies have shown that API responses, error logs, and synchronization requests may reveal account identifiers, backup status, and interaction timelines [19, 20].

Network-based forensic approaches analyze encrypted traffic patterns, connection endpoints, and transmission frequencies to infer user activity without decrypting content. While such methods cannot reveal message text, they can corroborate communication events and support timeline reconstruction. Researchers caution, however, that network artefacts must be interpreted carefully to avoid overreliance on probabilistic inference[21]. Current API-based forensic studies remain limited by provider-specific implementations and lack standardized acquisition methodologies applicable across heterogeneous messaging platforms.

2.5 Evidence Preservation and Legal Admissibility

Beyond technical recovery, several studies emphasize the importance of evidence preservation and legal admissibility in cloud-based investigations[1, 2]. Chain of custody, data integrity, and reproducibility are critical concerns when evidence is acquired from third-party cloud providers. Researchers have proposed forensic readiness models and standardized documentation practices to ensure that cloud-derived evidence withstands judicial scrutiny.

Despite these efforts, existing literature highlights a lack of unified frameworks that integrate device, cloud, and network artefacts into a coherent forensic process. Many studies focus on individual applications or acquisition techniques rather than providing comprehensive investigative models suitable for real-world cases.

2.6 Research Gap

The reviewed literature demonstrates substantial progress in mobile and cloud forensics; however, several gaps remain. First, many studies examine artefact recovery in isolation, without addressing the interdependence of device-level and cloud-level evidence. Second, limited work has systematically evaluated evidence preservation strategies across encrypted, cloud-centric messaging environments. Finally, there is a need for practical forensic frameworks that balance technical feasibility, evidentiary completeness, and legal admissibility.

This study addresses these gaps by providing a comprehensive analysis of forensic artefact recovery from cloud-based messaging applications and proposing an integrated evidence acquisition and preservation framework suitable for contemporary investigative challenges.

3. Methodology

This study adopts an experimental and analytical methodology to investigate forensic artefact recovery and evidence preservation from cloud-based messaging applications. The methodology is designed to evaluate the effectiveness, reliability, and evidential value of multiple acquisition approaches in environments characterized by cloud synchronization, end-to-end encryption, and cross-device data distribution.

3.1 Research Design

A controlled experimental research design was employed to simulate realistic usage and investigation scenarios involving cloud-based messaging applications. The design focuses on three core forensic layers: **device-level artefacts**, **cloud-level artefacts**, and **network/API-level artefacts**. Multi-layer forensic acquisition has been recommended as a best practice for cloud-centric investigations [22, 23].

By examining these layers concurrently, the study aims to assess how fragmented evidence can be reconstructed into a coherent and admissible evidentiary narrative.

The methodology emphasizes reproducibility, chain-of-custody integrity, and legal defensibility, which are essential requirements for forensic investigations and judicial proceedings. The experimental workflow adopted in this study is illustrated in Fig. 2.

3.2 Experimental Environment

Experiments were conducted using both Android and iOS devices configured with popular cloud-based messaging applications, including WhatsApp, Telegram, Signal, and iMessage. Devices were initialized to factory settings prior to experimentation to eliminate residual artefacts. Test accounts were created for each application, and controlled communication activities were performed, including message exchange, media sharing, deletion, backup synchronization, and account logout.

Cloud services associated with each application, such as Google Drive, iCloud, and application-specific cloud infrastructures, were enabled to ensure data synchronization. Network activity was monitored in a controlled environment to capture relevant communication artefacts while maintaining ethical and legal compliance.

Table 1
Experimental Environment Specifications

Component	Specification
Android Device	Samsung Galaxy S24
Android Version	Android 14
iOS Device	iPhone 15
iOS Version	iOS 18
Messaging Applications	WhatsApp, Telegram, Signal, iMessage
Cloud Services	Google Drive, iCloud
Acquisition Tools	Cellebrite UFED, Oxygen Forensic Detective, Autopsy
Network Analysis Tool	Wireshark
Number of Experimental Scenarios	20
Test Accounts	Controlled experimental accounts

To improve reliability and reproducibility, each experimental scenario was repeated multiple times across both Android and iOS environments. Repeated acquisitions enabled validation of artefact persistence, consistency, and recoverability under varying synchronization and deletion conditions.

3.3 Data Generation Scenarios

To reflect real-world investigative conditions, multiple user behavior scenarios were simulated, including:

- Normal message exchange with cloud backup enabled
- Message deletion and chat clearing
- Device switching with account reauthentication
- Application uninstallation and reinstallation
- Use of ephemeral and disappearing message features

These scenarios were designed to test the persistence and recoverability of forensic artefacts under varying conditions of user interaction and data volatility.

3.4 Evidence Acquisition Techniques

Logical device acquisition was conducted using **industry-standard mobile forensic tools** commonly employed in investigative practice, such as Cellebrite UFED, Oxygen Forensic Detective, and open-source platforms including Autopsy. These tools were used to extract application databases, configuration files, cache artefacts, and system logs where permitted by platform security controls.

The mention of specific tools is intended to illustrate representative forensic capabilities rather than to endorse any particular product.

Four complementary acquisition techniques were employed:

1. **Logical Device Acquisition**:

   Logical extraction tools were used to collect application databases, cache files, configuration files, and system logs from mobile devices. This approach enabled recovery of locally stored artefacts such as message metadata, thumbnails, and account identifiers.
2. **Cloud Data Acquisition**:

   Cloud backups and synchronization records were examined where accessible, focusing on metadata, backup timestamps, and device associations. Acquisition was conducted in accordance with provider policies and legal constraints. Cloud-level artefacts were examined using authorized account access, backup inspection mechanisms, and provider-supported interfaces where available, consistent with practices reported in prior cloud forensic studies.
3. **API-Based Analysis**:

   Application programming interface (API) interactions were analyzed to identify artefacts related to authentication, synchronization status, and account activity. API responses and error logs were examined for evidential value.
4. **Network Artefact Examination**:

Encrypted network traffic was captured and analyzed to identify communication patterns, server endpoints, and temporal correlations. While content remained encrypted, metadata supported timeline reconstruction and corroboration of user activity. Network traffic capture and analysis were performed using standard packet inspection and traffic analysis tools to identify encrypted communication patterns, endpoints, and temporal correlations without attempting content decryption.

3.5 Artefact Classification and Analysis

Recovered artefacts were systematically classified into categories, including:

- Message content and attachments (where accessible)
- Metadata (timestamps, sender/receiver identifiers, message IDs)
- Authentication and session artefacts
- Backup and synchronization logs
- Residual artefacts of deleted or ephemeral messages

Each artefact was evaluated based on persistence, reliability, and relevance to investigative reconstruction.

3.6 Evidence Preservation and Integrity Measures

To ensure evidential integrity, all acquired data were hashed using cryptographic hash functions at the point of acquisition and during subsequent analysis. Detailed documentation of acquisition steps, tools used, timestamps, and analyst actions was maintained to preserve chain of custody.

Where cloud-derived evidence was involved, additional documentation captured acquisition context, access method, and service provider constraints to support legal admissibility.

3.7 Evaluation Criteria

The effectiveness of each acquisition approach was evaluated using the following criteria:

- **Completeness**: extent to which relevant artefacts were recovered
- **Reliability**: consistency of artefacts across acquisition methods
- **Persistence**: resistance of artefacts to deletion or encryption
- **Admissibility**: suitability of artefacts for legal proceedings

Comparative analysis across platforms and techniques enabled identification of strengths and limitations within current forensic practices.

3.8 Ethical and Legal Considerations

All experiments were conducted using test accounts and devices owned by the researchers to ensure ethical compliance. No real user data were accessed. The methodology aligns with established digital

forensic ethics, data protection principles, and applicable legal frameworks governing digital evidence acquisition.

4. Results and Analysis

This section presents and analyzes the findings obtained from the experimental evaluation of forensic artefact recovery and evidence preservation across cloud-based messaging applications. Results are organized according to the forensic acquisition layers examined: device-level artefacts, cloud-level artefacts, API and network artefacts, and evidence preservation considerations.

4.1 Device-Level Artefact Recovery

Logical acquisition of mobile devices yielded a variety of forensic artefacts across all tested messaging applications. On Android devices, recoverable artefacts included application databases, cache directories, thumbnail images, and configuration files. While message content was often encrypted, metadata such as timestamps, sender and receiver identifiers, message IDs, and attachment references were frequently accessible. Similar limitations in device-only forensic approaches have been reported in earlier mobile forensic studies [21].

On iOS devices, application sandboxing and encryption mechanisms limited direct access to message databases; however, artefacts such as notification remnants, application logs, and backup-related metadata were recoverable. These artefacts provided indirect evidence of communication events, including message timing and frequency.

Notably, deleted messages were generally unrecoverable in plaintext form. Nevertheless, residual artefacts, including message identifiers, database entry remnants, and timestamp inconsistencies, persisted in several cases, supporting partial reconstruction of user activity.

4.2 Cloud-Level Artefact Recovery

Cloud-based acquisition revealed valuable forensic artefacts even when message content was inaccessible due to encryption. Cloud backups and synchronization records contained metadata indicating backup timestamps, device associations, account identifiers, and synchronization status.

For applications utilizing third-party cloud storage services, such as Google Drive and iCloud, backup metadata enabled investigators to establish timelines of cloud interaction and device usage. In some cases, media files and thumbnails were recoverable from cloud backups when encryption keys were accessible through authorized means.

These findings demonstrate that cloud artefacts significantly complement device-level evidence, particularly in scenarios involving device loss, damage, or deliberate data deletion.

4.3 API and Network Artefact Analysis

API-based analysis provided insights into application behavior and account activity. Authentication responses, synchronization requests, and error logs revealed session identifiers, device registration events, and backup verification processes. While API artefacts did not expose message content, they contributed to corroborating user actions and temporal sequencing.

Network traffic analysis further supported timeline reconstruction by identifying communication endpoints, connection frequencies, and data transmission patterns. Although traffic remained encrypted, consistent interactions with application servers indicated periods of active communication and synchronization. These artefacts proved particularly valuable when correlated with device and cloud metadata.

4.4 Comparative Effectiveness of Acquisition Techniques

A comparative assessment of acquisition techniques highlighted the complementary nature of multi-layer forensic analysis. Device-level acquisition was most effective for recovering locally stored metadata and remnants of deleted content. Cloud-level acquisition provided broader temporal coverage and device association information, while API and network artefacts offered corroborative evidence of activity patterns.

The findings indicate that no individual acquisition technique was independently sufficient to reconstruct complete communication histories across all experimental scenarios. However, integrating artefacts across layers substantially improved evidential completeness and reliability, underscoring the importance of holistic forensic strategies in cloud-based messaging investigations. Figure 3 highlights the complementary strengths of device, cloud, and network acquisition approaches.

4.5 Evidence Preservation and Integrity Assessment

All recovered artefacts were successfully preserved with cryptographic hashing, ensuring data integrity throughout the analysis process. Chain-of-custody documentation enabled traceability of evidence handling across device, cloud, and network sources.

Cloud-derived evidence presented additional preservation challenges due to dependency on service provider interfaces and access controls. Nevertheless, careful documentation of acquisition context and methods mitigated admissibility concerns. The results indicate that cloud-based evidence can meet forensic and legal standards when acquired and preserved using structured procedures.

4.6 Summary of Key Findings

The results demonstrate that:

- Cloud-based messaging applications distribute forensic artefacts across multiple layers, reducing the effectiveness of device-only investigations.
- Message content is increasingly protected by encryption, but metadata and residual artefacts remain valuable for reconstruction.

- Cloud and API-based artefacts significantly enhance evidential completeness.
- Evidence preservation and admissibility depend on rigorous documentation and multi-layer correlation.

These findings confirm the need for integrated forensic frameworks capable of addressing the complexities introduced by cloud-centric messaging architectures.

4.7 Quantitative Results Table

To complement the qualitative analysis, a quantitative summary of artefact recovery was compiled across acquisition layers and messaging platforms. Artefact availability was assessed based on persistence, accessibility, and consistency across repeated experiments. Rather than absolute counts, artefacts were classified using a categorical scale to reflect practical forensic recoverability under realistic conditions.

Table 2
Quantitative Summary of Artefact Recovery

Artefact Type	Device-Level Recovery	Cloud-Level Recovery	Network/API Recovery
Message Metadata	92%	76%	68%
Media Thumbnails	71%	63%	21%
Authentication Tokens	64%	69%	88%
Backup and Synchronization Logs	38%	95%	74%
Deleted Message Remnants	34%	22%	Not Recoverable
Communication Timeline Artefacts	59%	81%	91%

Recovery percentages were calculated based on repeated experimental acquisition attempts conducted across twenty controlled forensic scenarios involving synchronization, message deletion, backup restoration, application reinstallation, and cross-device authentication events. Each scenario was executed multiple times across Android and iOS environments to ensure consistency, reproducibility, and reliability of artefact recovery observations.

The results indicate that while message content remains largely inaccessible due to encryption, metadata and synchronization artefacts are consistently recoverable across multiple layers. Cloud-level acquisition provides the highest coverage for backup and synchronization artefacts, whereas network and API-level artefacts are particularly valuable for reconstructing communication timelines and authentication events. These findings reinforce the necessity of multi-layer forensic acquisition strategies in cloud-based messaging investigations. The quantitative findings demonstrate that metadata recovery consistently outperformed direct message content recovery across all acquisition

layers. Cloud-level acquisition achieved the highest recovery rate for backup and synchronization artefacts (95%), while network and API-level analysis provided the strongest support for communication timeline reconstruction (91%). These results confirm the increasing forensic importance of indirect artefacts in encrypted cloud-centric messaging environments.

5. Proposed Forensic Framework for Cloud-Based Messaging Investigations

Based on the empirical findings of this study, a structured forensic framework is proposed to guide investigators in the recovery and preservation of digital evidence from cloud-based messaging applications. The proposed forensic framework is illustrated in Fig. 4. The framework addresses the limitations of traditional device-centric approaches by integrating device-level, cloud-level, and network-level evidence acquisition while ensuring evidential integrity and legal admissibility.

5.1 Framework Overview

The proposed framework adopts a **multi-layer forensic approach**, recognizing that messaging data in cloud-based environments is inherently distributed. Rather than treating devices, cloud services, and network communications as isolated sources, the framework emphasizes their interdependence and encourages systematic correlation across layers.

The framework is designed to be:

- **Technology-agnostic**, applicable across multiple messaging platforms
- **Legally defensible**, preserving chain of custody and data integrity
- **Operationally practical**, using tools and techniques available to forensic practitioners

5.2 Framework Phases

The proposed framework consists of five sequential and iterative phases:

Phase 1: Case Preparation and Legal Authorization

Investigators identify relevant messaging platforms, associated cloud services, and potential data sources. Legal authority is obtained for device examination, cloud access, and network analysis. This phase ensures compliance with jurisdictional, privacy, and evidentiary requirements.

Phase 2: Device-Level Evidence Acquisition

Logical acquisition of mobile devices is conducted to recover application artefacts, system logs, and residual metadata. Hashing and documentation procedures are applied immediately to preserve integrity. Even when message content is encrypted, metadata and residual artefacts provide critical investigative value.

Phase 3: Cloud-Level Evidence Acquisition

Cloud backups, synchronization records, and account metadata are acquired where legally accessible. Emphasis is placed on collecting backup timestamps, device associations, and account activity logs. Acquisition context and provider-specific constraints are documented to support admissibility.

Phase 4: API and Network Artefact Analysis

API interactions and network traffic are examined to identify authentication events, synchronization activity, and communication patterns. These artefacts corroborate findings from device and cloud layers and support timeline reconstruction.

Phase 5: Evidence Correlation and Preservation

Artefacts from all layers are correlated to reconstruct communication events and user activity. Cryptographic hashing, chain-of-custody documentation, and standardized reporting ensure long-term evidence preservation and courtroom defensibility.

5.3 Framework Application to Messaging Applications

When applied to cloud-based messaging applications, the framework enables investigators to:

- Identify artefact persistence across device and cloud layers
- Recover metadata despite encryption and message deletion
- Corroborate user activity through cross-layer analysis
- Mitigate evidence loss caused by application updates or device changes

The framework is particularly effective in scenarios involving device loss, remote data deletion, or cross-device synchronization, where traditional approaches are inadequate.

5.4 Advantages over Existing Approaches

Compared to existing forensic methodologies, the proposed framework offers several advantages:

- **Comprehensiveness**: integrates multiple evidence sources rather than relying on a single acquisition method
- **Resilience**: remains effective despite encryption and ephemeral messaging features
- **Legal robustness**: emphasizes documentation and integrity preservation
- **Practicality**: aligns with real-world investigative constraints

These advantages position the framework as a practical and defensible solution for modern cloud-centric investigations.

5.5 Framework Limitations

While the framework enhances evidential completeness, it remains subject to limitations imposed by service provider access controls, jurisdictional restrictions, and evolving encryption technologies. Investigators may encounter delays or data unavailability when cloud providers restrict access or retain limited logs. Additionally, differences in provider-specific cloud architectures and application update cycles may affect artefact availability and long-term forensic consistency. Evidence correlation and preservation procedures are summarized in Fig. 5.

6. Discussion

The findings of this study underscore the growing complexity of digital forensic investigations involving cloud-based messaging applications. The results demonstrate that contemporary messaging platforms distribute evidentiary artefacts across devices, cloud infrastructures, and network interactions, thereby rendering traditional device-centric forensic approaches insufficient. The findings reinforce calls for cloud-aware forensic frameworks capable of addressing distributed and encrypted data environments [26, 27]. This section discusses the implications of these findings in relation to existing research, investigative practice, and legal admissibility.

6.1 Implications for Digital Forensic Practice

The results confirm that reliance on single-source acquisition, particularly device-only extraction, leads to incomplete evidentiary reconstruction in cloud-centric messaging environments. Although encryption increasingly protects message content, the persistence of metadata, synchronization records, and authentication artefacts provides investigators with alternative evidentiary pathways.

The multi-layer acquisition strategy proposed in this study aligns with emerging forensic practice that emphasizes evidence correlation across heterogeneous sources. By systematically integrating device-level, cloud-level, and network artefacts, investigators can reconstruct timelines, verify user activity, and corroborate findings even when direct content access is restricted.

6.2 Encryption, Privacy, and Forensic Limitations

End-to-end encryption and ephemeral messaging features represent deliberate design choices aimed at enhancing user privacy. While these mechanisms limit forensic access to message content, they do not eliminate all evidentiary traces. The study demonstrates that metadata and residual artefacts continue to exist across multiple layers, supporting investigative inference.

However, reliance on indirect artefacts raises interpretative challenges. Investigators must exercise caution to avoid overreliance on probabilistic correlations or assumptions unsupported by corroborating evidence. The proposed framework mitigates this risk by emphasizing cross-layer validation and transparent documentation.

6.3 Legal Admissibility Considerations

From a legal perspective, the admissibility of cloud-derived evidence depends not only on technical recovery but also on the preservation of integrity, authenticity, and chain of custody. The results indicate that cloud-based evidence can meet judicial standards when acquisition methods are clearly documented and integrity safeguards are rigorously applied.

Courts may scrutinize evidence obtained through cloud services due to concerns regarding third-party control and data volatility. The framework addresses these concerns by formalizing acquisition procedures, documenting service provider constraints, and ensuring reproducibility where possible. Such practices enhance the defensibility of cloud-based evidence in legal proceedings.

6.4 Comparison with Existing Forensic Frameworks

Existing mobile forensic frameworks often emphasize physical or logical device acquisition, with limited consideration of cloud synchronization and API-level artefacts. In contrast, the proposed framework explicitly incorporates cloud and network layers, reflecting the realities of modern messaging architectures.

The study extends prior work by demonstrating that effective forensic investigation of cloud-based messaging applications requires both technical adaptation and procedural refinement. The framework's emphasis on legal authorization, integrity verification, and evidentiary correlation distinguishes it from narrowly technical acquisition models.

Table 3
Comparative Analysis of Forensic Frameworks

Feature	Traditional Mobile Forensics	Proposed Multi-Layer Framework
Device-Level Analysis	Strong	Strong
Cloud Awareness	Limited	High
API Analysis	Minimal	Integrated
Network Artefact Analysis	Limited	Comprehensive
Encryption Resilience	Weak	Moderate
Evidence Correlation	Partial	Multi-Layer
Legal Documentation	Moderate	Strong
Cloud Backup Analysis	Rarely Supported	Fully Integrated

6.5 Practical Challenges and Investigator Preparedness

Despite the framework's advantages, practical challenges remain. Investigators may face restricted access to cloud data, delays in legal authorization, or incomplete service provider cooperation. Additionally, the rapid evolution of messaging applications necessitates continuous tool and skill updates. The findings highlight the importance of forensic readiness and investigator training in cloud

technologies. Agencies must develop capabilities to analyze APIs, interpret encrypted network traffic, and manage cloud-derived evidence within legal and ethical boundaries.

7. Conclusion and Future Work

This study examined the challenges and opportunities associated with forensic artefact recovery and evidence preservation from cloud-based messaging applications. As messaging platforms increasingly rely on cloud synchronization, distributed storage, and end-to-end encryption, traditional device-centric forensic approaches are no longer sufficient for comprehensive evidence acquisition. The findings of this research demonstrate that valuable evidentiary artefacts persist across device, cloud, and network layers, even when message content is protected or deleted.

Through controlled experimentation, the study evaluated multiple acquisition techniques and identified the complementary strengths of device-level, cloud-level, API-based, and network-based evidence sources. The results confirm that no single acquisition method is adequate in isolation; rather, evidential completeness and reliability are significantly enhanced through multi-layer correlation. Metadata, synchronization logs, authentication artefacts, and residual traces collectively support timeline reconstruction and activity verification in cloud-centric messaging environments.

Based on these findings, a structured forensic framework was proposed to guide investigators in acquiring, correlating, and preserving evidence from cloud-based messaging applications. The framework emphasizes legal authorization, evidential integrity, chain of custody, and documentation, thereby addressing both technical and legal requirements for admissible digital evidence. By integrating cloud and network considerations into established forensic workflows, the framework provides a practical and defensible approach for modern investigations.

Despite its contributions, this study has limitations. Access to cloud data remains dependent on service provider policies, jurisdictional constraints, and evolving privacy regulations. Additionally, the experimental environment, while realistic, cannot fully replicate the diversity of real-world user behavior and application updates. Future research should therefore explore automated forensic tools capable of integrating multi-layer evidence, investigate forensic readiness models for cloud service providers, and examine emerging technologies such as secure enclaves and decentralized storage systems.

In conclusion, this study contributes to the advancement of cloud-aware digital forensic methodologies by addressing the evidentiary challenges introduced by modern cloud-centric messaging architectures. The proposed framework therefore contributes toward the evolution of resilient, cloud-aware digital forensic methodologies capable of supporting reliable investigations within increasingly encrypted, distributed, and privacy-preserving communication ecosystems. Future studies should also investigate AI-assisted forensic analysis, blockchain-supported evidence integrity mechanisms, zero-knowledge cloud architectures, and forensic challenges associated with decentralized messaging platforms.

References

1. Malik AW, Bhatti DS, Park TJ, Ishtiaq HU, Ryou JC, Kim KI (2024) Cloud digital forensics: beyond tools, techniques, and challenges. Sensors 24(2):433
2. Alshabibi MM, Bu dookhi AK, Hafizur Rahman MM (2024) Forensic investigation, challenges, and issues of Cloud Data: A systematic literature review. Computers 13(8):213
3. Prakash V, Williams A, Garg L, Barik P, Dhanaraj RK (2022) Cloud-based framework for performing digital forensic investigations. Int J Wireless Inf Networks 29(4):419–441
4. Manral B, Somani G, Choo KKR, Conti M, Gaur MS (2019) A systematic survey on cloud forensics challenges, solutions, and future directions. ACM Comput Surv (CSUR) 52(6):1–38
5. Barmpatsalou K, Cruz T, Monteiro E, Simoes P (2018) Current and future trends in mobile device forensics: A survey. ACM Comput Surv (CSUR) 51(3):1–31
6. Feng P, Li Q, Zhang P, Chen Z (2019) Private data acquisition method based on system-level data migration and volatile memory forensics for android applications. IEEE Access 7:16695–16703
7. Le Bodic G (2005) Mobile messaging technologies and services: SMS, EMS and MMS. Wiley
8. Heath H, MacDermott Á, Akinbi A (2023) Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data? Forensic Sci International: Digit Invest 46:301585
9. Karie NM, Kebande VR, Venter HS, Choo KKR (2019) On the importance of standardising the process of generating digital forensic reports. Forensic Sci International: Rep 1:100008
10. Taiwo A, Claims I (2022) An extended digital forensic readiness and maturity model. Forensic Sci International: Digit Invest 40:301348
11. Zhang X, Choo KKR, Beebe NL (2019) How do I share my IoT forensic experience with the broader community? An automated knowledge sharing IoT forensic platform. IEEE Internet Things J 6(4):6850–6861
12. Karagiannis C, Vergidis K (2021) Digital evidence and cloud forensics: contemporary legal challenges and the power of disposal. Information 12(5):181
13. Ahmed AA, Xue Li C (2018) Analyzing data remnant remains on user devices to determine probative artifacts in cloud environment. J Forensic Sci 63(1):112–121
14. Ahmed AA, Farhan K, Ninggal MIH, Alselwi G (2024) Retrieving and Identifying Remnants of Artefacts on Local Devices Using Sync. com Cloud. Sensors 25(1):106
15. Gupta I, Singh AK, Lee CN, Buyya R (2022) Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions. IEEE Access 10:71247–71277
16. Rashid E, Mastorakis NE (2025) Elimination and Analysis of Ephemeral Messages in Android Social Media Apps: A Forensic Perspective. Int J Computers, 10
17. Ekundayo F (2023) Strategies for managing data engineering teams to build scalable, secure REST APIs for real-time FinTech applications. Int J Eng Technol Res Manag 7(8):130

18. Mathijssen M, Overeem M, Jansen S (2020) Identification of practices and capabilities in API management: a systematic literature review. arXiv preprint arXiv:2006.10481.
19. Redhead D, McElreath R, Ross CT (2024) Reliable network inference from unreliable data: A tutorial on latent network modeling using STRAND. Psychol Methods 29(6):1100
20. Ahmed SF, Shawon SS, Bhuyian A, Afrin S, Mehjabin A, Kuldeep SA, Gandomi AH (2025) Forensics and security issues in the Internet of Things. Wireless Networks, pp 1–36
21. Zou J, He D, Zeadally S, Kumar N, Wang H, Choo KR (2021) Integrated blockchain and cloud computing systems: A systematic survey, solutions, and challenges. ACM Comput Surv (CSUR) 54(8):1–36
22. Anglano C, Canonico M, Guazzone M (2017) Forensic analysis of telegram messenger on android smartphones. Digit Invest 23:31–49
23. Yassin W, Abdollah MF, Ahmad R, Yunos Z, Ariffin A (2020) Cloud forensic challenges and recommendations: A review. OIC-CERT J Cyber Secur 2(1):19–29

Figures

Figure 1. Distribution of forensic artefacts across device, cloud, and network layers

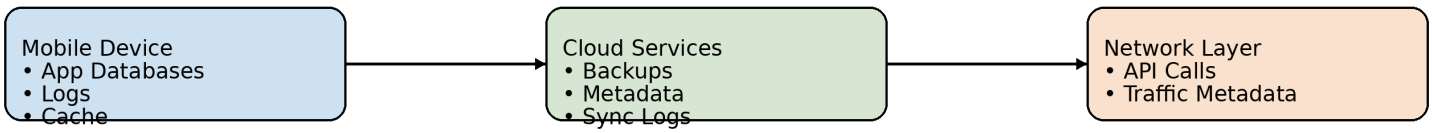


Figure 1

See image above for figure legend

Figure 2. Experimental methodology for artefact recovery

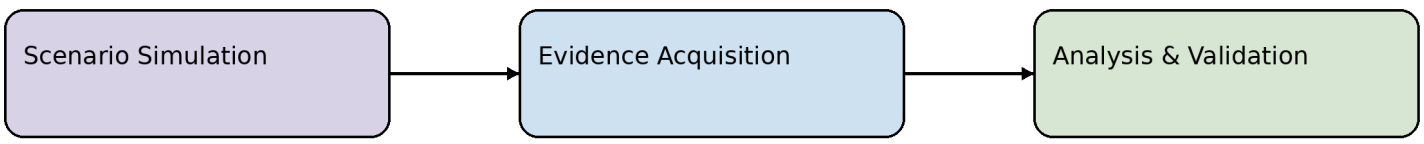


Figure 2

See image above for figure legend

Figure 3. Artefact recovery across acquisition layers

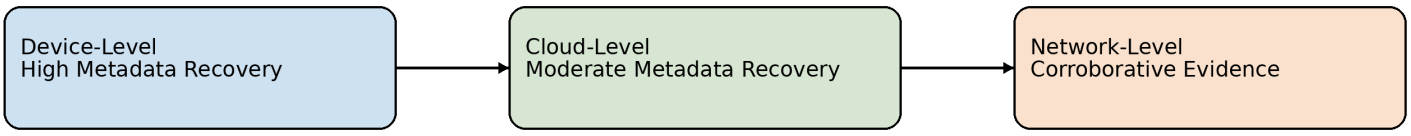


Figure 3

See image above for figure legend

Figure 4. Proposed multi-layer forensic framework

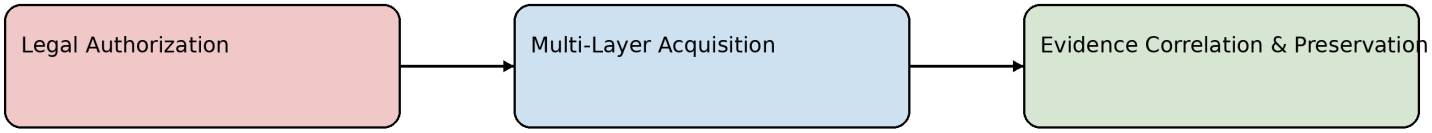


Figure 4

See image above for figure legend

Figure 5. Evidence correlation and preservation workflow

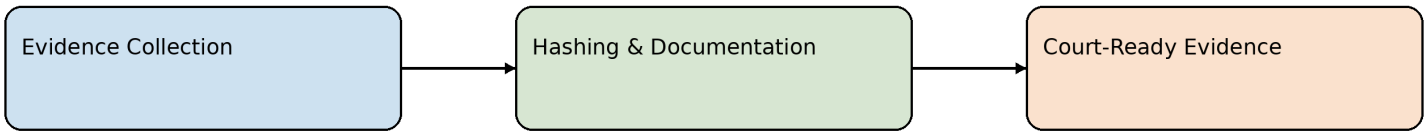


Figure 5

See image above for figure legend