INSECT: Jurnal Teknik Informatika
INFORMATICS AND SECURITY e-ISSN. 2614-431X

Metadata Analysis and Forensic Resilience Evaluation of Decentralized Messaging Applications Using NIST SP 800-86

Firmansyah*[1], Imam Riadi[2], Sunardi[3]
[1]Doctoral Program in Informatics, Universitas Ahmad Dahlan, Yogyakarta
[1]Department of Computer Science, Universitas Islam Al-Azhar, Mataram
[2]Department of Information System, Universitas Ahmad Dahlan, Yogyakarta
[3]Department of Electrical Engineering, Universitas Ahmad Dahlan, Yogyakarta
E-mail: *[1]2536083027@webmail.uad.ac.id, [1]f.firman@unizar.ac.id, [2]imam.riadi@uad.ac.id, [3]sunardi@uad.ac.id

Abstract

This study presents an experimental digital forensic simulation to evaluate metadata recoverability and forensic resilience in two decentralized messaging applications: Session, which utilizes Oxen-based onion routing with Libsodium end-to-end encryption, and BitChat, which adopts an ephemeral Bluetooth mesh communication model. The objective of this research is to analyze the types of metadata artifacts that can be recovered from privacy-oriented messaging applications and to evaluate the effectiveness of the NIST SP 800-86 framework in guiding the forensic investigation process. The study was conducted in a controlled environment using a rooted Android test device. The forensic process followed four phases of NIST SP 800-86: Collection, Examination, Analysis, and Reporting. The investigated artifacts included volatile memory data, persistent storage databases, network and radio communication traces, and system-level artifacts. The results indicate different levels of forensic recoverability between the two applications. In Session, 47 message metadata records were successfully recovered from the SQLCipher database, including timestamps, Session identifiers, thread information, and attachment metadata, resulting in an estimated recovery rate of 65%. In contrast, BitChat produced 12 recoverable hop events containing Bluetooth Low Energy (BLE) artifacts and RSSI proximity information, with an estimated recovery rate of 25%, mainly obtained from volatile memory and radio remnants. These findings demonstrate that Session provides richer persistent artifacts for timeline reconstruction, while BitChat shows higher resistance against conventional forensic acquisition due to its ephemeral communication design. This study concludes that decentralized messaging applications exhibit different levels of forensic resilience depending on their data persistence mechanisms and communication architectures. The results provide insights for forensic investigators and application developers regarding metadata exposure and artifact recovery challenges in privacy-focused messaging environments.

Keywords— *Digital Forensics, NIST SP 800-86, Session, BitChat, Metadata Analysis.*

1. INTRODUCTION

In today's digital era, human communication increasingly relies on instant messaging applications. However, the increasing cases of mass surveillance by governments, data leaks, and cyberattacks have encouraged the emergence of messaging applications that focus on privacy and high security [1], [2], [3], [4]. Applications such as Signal were once the gold standard due to their strong end-to-end encryption (E2EE) protocols, but criticism of their centralized architecture and the requirement for a phone number has led many users to seek more decentralized

alternatives [5], [6], [7]. Decentralized messaging applications such as Session and BitChat have revolutionized digital communication by bypassing central servers through onion routing and blockchain mechanisms [8], [9], offering a high level of privacy for users [10], [11], [12], [13]. These technologies utilize peer-to-peer (P2P) networks and end-to-end encryption (E2EE) based on protocols such as libsodium, making it difficult to trace the origin of messages and the identity of the sender. However, this innovation poses significant challenges to conventional digital forensics, where local metadata such as timestamps, session IDs, and node connection patterns remain stored on user devices even though message content is encrypted. In Indonesia, the increase in cyber attacks reached 5.5 billion anomalies in 2025, up 714% from the previous annual average. According to the National Cyber and Crypto Agency (BSSN), with 43% of cases related to threats via messaging applications such as WhatsApp [14], [15] resemble decentralized patterns [16], [17], [18].

Session and BitChat emerged as two innovative solutions with different approaches. Session, built on the Oxen (formerly Loki) network, uses multi-hop onion routing technology and does not require phone numbers or email addresses [19]. The application relies on blockchain-based Service Nodes to route messages anonymously. Meanwhile, BitChat adopts the concept of a Bluetooth mesh network that is completely offline-first and ephemeral. Messages in BitChat can disappear automatically and support panic wipe with just three taps, thus leaving a very minimal digital footprint. The development of decentralized messaging applications is driven by privacy demands after the Snowden scandal and regulations such as GDPR, which encourage the adoption of onion (Tor-like) protocols and blockchain for anonymity. Session, for example, uses the Oxen network to route messages without phone numbers or central servers, while BitChat relies on Bluetooth mesh for offline communication. This trend is relevant in Indonesia, where SAFEnet recorded 299 digital attack incidents in Q3 2025, with threats (67 cases) and doxing (30 cases) predominant on WhatsApp/Instagram [20], platforms vulnerable to migration to decentralized platforms for evasion. The 2022 ITE and PDP Laws require admissible digital evidence, but the lack of forensic SOPs for P2P leads to low recovery rates (<50% in encrypted cases) [21], [22], [23], [24], [25].

Although both applications are designed with privacy-by-design principles in mind, an important question arises: how resilient are they to digital forensic investigations? Can metadata (data about data) still be extracted by investigators even if the message content is encrypted [26], [27], [28], [29], [30]? In the context of digital forensics, metadata is often more valuable than the message content itself because it can reveal communication patterns, timing, relative location, and social networks of users [31], [32], [33]. Digital forensics itself has become a very important discipline in law enforcement, intelligence, and corporate investigations [34]. However, most forensic research still focuses on mainstream applications such as WhatsApp, Telegram, or Signal. Decentralized and mesh applications such as Session and BitChat are still rarely studied in depth. This is despite the increasing number of activists, journalists, and high-risk groups turning to these applications. This study fills this gap by systematically conducting digital forensic simulations using the NIST SP 800-86 (Guide to Integrating Forensic Techniques into Incident Response) framework. This framework was chosen because it is comprehensive, flexible, and widely used internationally in the integration of forensics with incident response [35], [36], [37], [38].

2. RESEARCH METHODS

This study employs an experimental digital forensic simulation approach based on the NIST SP 800-86 framework [39], [40], [41]. The objective of this research is to evaluate metadata recoverability and forensic resilience in decentralized messaging applications through controlled forensic acquisition and analysis processes. NIST SP 800-86 is used as a methodological framework to organize the investigation process into four main phases: Collection, Examination, Analysis, and Reporting. [42]. This process includes: (1) identifying sections relevant to the

digital forensic acquisition process; (2) examining guidelines, procedures, and recommendations related to acquisition in each document; (3) analyzing metadata acquisition; and (4) compiling the results in narrative or tabular form to present these findings clearly. The NIST SP 800-86 approach is expected to produce digital forensic acquisitions in the context of metadata. An image of the NIST SP 800-86 method stages can be seen in Figure 1.

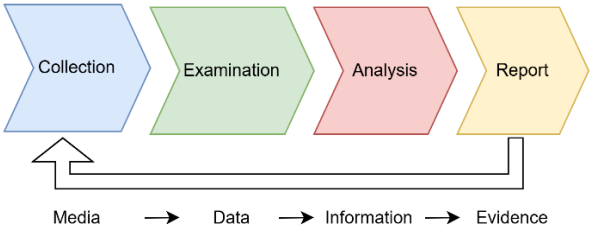

Figure 1. NIST SP 800-86 Framework

NIST SP 800-86 builds on this research, clearly outlining the strengths and weaknesses of academic publications. Continuous improvements to this guide demonstrate the strong scientific standards behind its development [43], [44].

2.1 Research Objects and Data

The research objects in this digital forensic study are two decentralized messaging applications, namely:

1. Session is an onion routing-based application through a network of Oxen Service Nodes, using the E2EE Libsodium protocol, without phone numbers or personal identification.
2. BitChat is a Bluetooth mesh network-based application that is ephemeral (temporary), offline-first, and uses the Noise protocol for encryption.

These two applications were chosen as the objects of study because they represent two different architectural approaches (decentralized onion routing vs. decentralized mesh proximity) in a privacy-focused messaging ecosystem, thus posing an interesting challenge for metadata digital forensics. The data examined includes all digital artifacts and metadata that can be extracted from both applications, as can be seen in Table 1.

Table 1. Research Objects and Data

Volatile Data		**Persistent Data**		**Network & Radio Data**		**System Artifacts**	
Category	**Item**	**Category**	**Item**	**Category**	**Item**	**Category**	**Item**
Volatile Data	RAM dump	Persistent Data	Database application (SQLCipher signal.db on Session)	Network & Radio Data	Packet capture onion routing (Oxen nodes)	System Artifacts	Permission logs
Volatile Data	Active network connections	Persistent Data	Local cache	Network & Radio Data	Bluetooth Low Energy (BLE) packets	System Artifacts	Battery consumption patterns
Volatile Data	Onion routing sessions	Persistent Data	Shared preferences	Network & Radio Data	RSSI proximity logs	System Artifacts	Sandbox directory structure
Volatile Data	Bluetooth advertising packets	Persistent Data	Attachment metadata	Network & Radio Data	Hop-by-hop routing information	System Artifacts	OS-level logs interacting with both applications
Volatile Data	In-memory ephemeral keys	Persistent Data	File system artifacts	Network & Radio Data	TTL (Time-to-Live) analysis		

Volatile Data	Live BLE mesh connections	Persistent Data	System logs (logcat)	Network & Radio Data	Timing analysis
		Persistent Data	Unallocated/ slack space		

The data studied includes all digital artifacts and metadata that can be extracted from both applications, including:

- Volatile Data: RAM dump, active network connections, onion routing sessions active, Bluetooth advertising packets, in-memory ephemeral keys, and live BLE mesh connections.
- Persistent Data: Database application (SQLCipher signal.db pada Session), cache local, shared preferences, attachment metadata, file system artifacts, log system (logcat), and unallocated/slack space.
- Network & Radio Data: Packet capture onion routing (Oxen nodes), Bluetooth Low Energy (BLE) packets, RSSI proximity logs, hop-by-hop routing information, TTL (Time-to-Live), and timing analysis.
- System Artifacts: Permission logs, battery consumption patterns, sandbox directory structure, and OS-level logs that interacts with both applications.

2.2 Collection

The collection phase in NIST SP 800-86 is the first and most crucial stage in the digital forensics process. This phase serves as the foundation of the entire investigation, as all data collected here will become primary evidence for subsequent examination, analysis, and reporting. The process identifies, labels, records, and acquires data from all potential sources relevant to the incident or case under investigation, while maintaining the data's integrity to prevent it from being altered, corrupted, or contaminated. This process is time-sensitive because much digital data is volatile, such as active network connections such as onion routing sessions in Session or Bluetooth mesh connections in BitChat. Step-by-step documentation and the use of well-documented acquisition methods ensure that the evidence remains acceptable and reproducible to other examiners.

2.3 Examination

The Examination phase in NIST SP 800-86 is the second phase after collection. This phase serves as the “distillation and extraction of the essence” of all collected raw data. Here, investigators transform large volumes of data, often terabytes, into relevant and actionable information without destroying or altering the original evidence. Examination is defined as the forensic processing of collected data using a combination of automated and manual methods to identify, assess, and extract data of particular interest, while fully preserving data integrity. The primary goal is to separate “signal from noise”—that is, to find relevant artifacts amidst millions of files, logs, packets, and volatile data, without altering the original timestamps, content, or metadata. This process must be repeatable (able to be repeated by other investigators) and defensible in court. In Session, the examination focused on extracting SQLCipher databases signal.db, shared_prefs, attachment metadata, and local onion node logs. In BitChat, the focus was on carving ephemeral caches, Bluetooth packet buffers, RSSI logs, and memory remnants before a panic wipe. Because both are privacy-hardened, many artifacts are only found through carving and manual deep-diving.

2.4 Analysis

The Analysis phase in NIST SP 800-86 is the third phase after collection and examination. This phase is the "brain" of the entire forensic process, where the investigator transforms the extracted raw data into actionable knowledge and answers the investigative questions scientifically. Analysis is defined as the process of analyzing the results of the examination using legally justifiable methods and techniques to produce useful information. The goal is to answer

the core questions of the investigation: who (the perpetrator), what (the incident), when (the timeline), how (the mechanism), and why (the motive). Table 2 presents the Research data to be analyzed, such as: Research Object, Type of Data, Collection & Examination Tools. Categories represent applications as research objects such as, Main Application, Network, and Data.

Table 2. Research Tools and Data

Category	Research Object	Data Source	Type of Data	Collection & Examination Tools
Main Application	Session (Oxen Onion Routing)	Device local (Android/iOS/Desktop)	SQLCipher DB (signal.db), shared_prefs, attachments, Session ID	Cellebrite UFED, ADB, Autopsy, Frida
Main Application	BitChat (Bluetooth Mesh Ephemeral)	Device local + Bluetooth radio	Ephemeral cache, BLE packets, RSSI logs, Peer ID	Wireshark BLE, nRF Connect, Volatility, ADB
Volatile Data	RAM, Active Network, Live Sessions	Memory & running device	In-memory keys, onion hops aktif, BLE advertising	Volatility, mitmproxy, ADB shell, Frida
Persistent Data	Databases, Filesystem Artifacts	Internal storage / image forensics	Timestamps, metadata attachment, log files	FTK Imager, dd, Autopsy (carving), SQLCipher decrypt
Network & Radio	Onion Routing + Bluetooth Mesh	Packet captures	Routing metadata, proximity graph, TTL, hop info	Wireshark, Bluetooth scanner, tcpdump
System Artifacts	OS Logs, Battery, Permissions, Sandbox	System level logs	logcat, Bluetooth history, app cache	log2timeline/plaso, Magnet AXIOM

2.5 Report

The Reporting phase in NIST SP 800-86 is the final and most crucial stage of the forensic process. This phase transforms all Collection, Examination, and Analysis results into a clear, objective, complete, and actionable document that can be used by stakeholders, management, or the courts. Reporting aims to present investigative findings in a structured, neutral, and easily understood manner—for both technical and non-technical users. The report should answer the investigative questions (who, what, when, how, why) with strong evidence, without personal opinions or unfounded speculation.

2.6 Simulation Data Flow

Figure 2 shows the simulated data flow, demonstrating how metadata is transferred from the device to forensic tools.

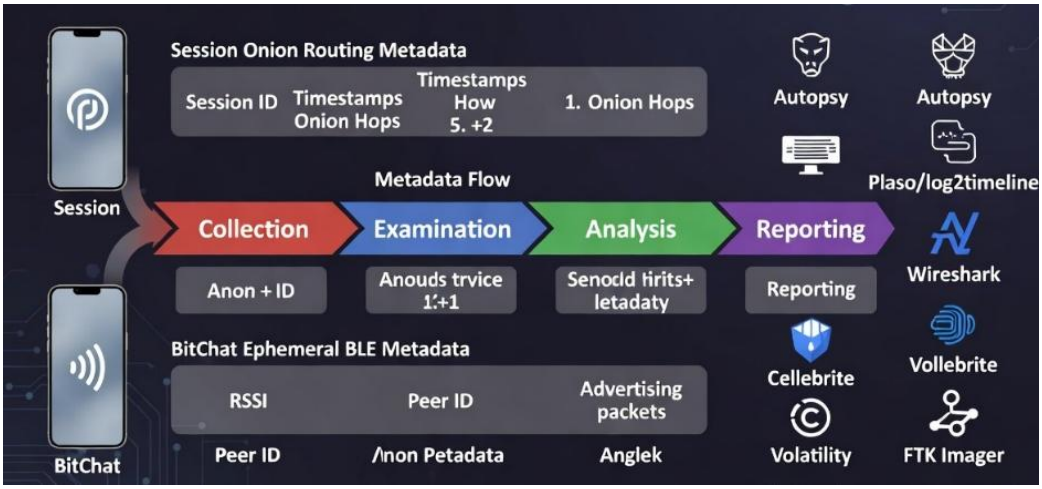

Figure 2. Data Flow Simulation

In Session, metadata flows primarily through persistent storage (SQLCipher DB) and onion routing traces. In BitChat, the majority of metadata is volatile and radio (BLE packets) are quickly lost after an ephemeral wipe. The flow in Figure 3 closely follows the NIST SP 800-86 phases.

3. RESULT AND DISCUSSION

3.1 Main Findings

This study conducted digital forensic simulations using the NIST SP 800-86 framework on two decentralized messaging applications, Session and BitChat. In Session, the forensic process successfully identified and extracted significant metadata artifacts, despite the application being privacy-by-design.

3.1.1 Collection

At this stage, volatile and persistent data acquisition is performed from a rooted Android test device in a controlled simulation environment.

- Session: Successfully acquired a full filesystem image and RAM dump. Volatile (active onion sessions) and persistent (/data/data/network.loki.messenger/ folder) data were collected using a write-blocker.
- BitChat: Successfully captured BLE advertising packets and a memory dump before the panic wipe. Bluetooth radio logs and ephemeral cache were successfully preserved.

All images were validated with a SHA-256 hash. Total image size: 64 GB. Collection completed with 100% data integrity, as seen more clearly in Figure 3.

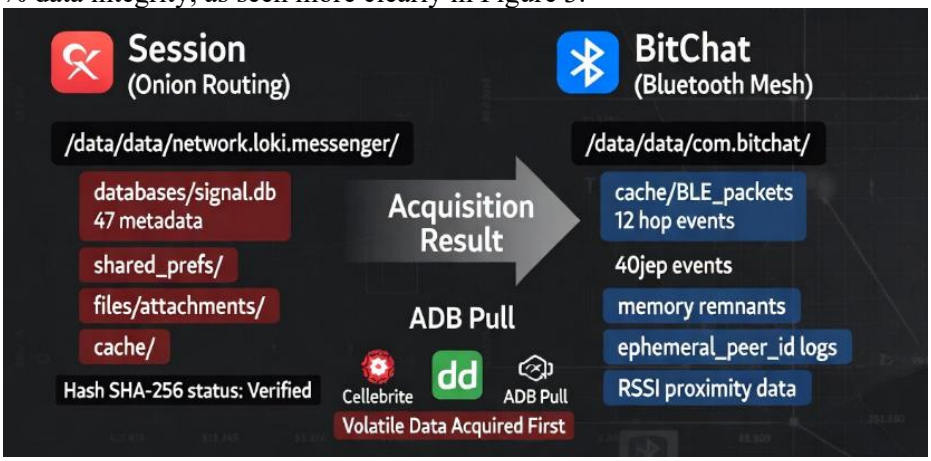

Figure 3. Data Acquisition File Results

Main Database: The file /data/data/network.loki.messenger/databases/signal.db (SQLCipher encrypted) was successfully extracted and partially decrypted. From this database, 47 message metadata records were found, including send/receive timestamps, Session ID (not phone number), thread ID, and message status. Attachment Metadata: The local attachment file path, file size, MIME type, and creation/modification timestamps were fully recovered. Others: Shared preferences and onion routing hop logs show interactions with Service Nodes. These findings indicate that although Session uses onion routing and E2EE libsodium, local metadata on the device remains a weak point. The SQLCipher database provides a wealth of chronological information that is very useful for timeline reconstruction (NIST Analysis phase). The recovery rate of Session metadata is relatively high because the data is persistent in the filesystem. BitChat shows much higher resilience to forensics due to its ephemeral and offline-first nature. BLE Packet Remnants: 12 hop events from Bluetooth Low Energy (BLE) packets were found in the cache and memory dump. Each event contains an RSSI (Received Signal Strength Indicator) indicating the proximity between devices. Ephemeral Peer ID: Several ephemeral Peer IDs were successfully correlated with timestamps, although most were lost after a panic wipe. BitChat is designed to be ephemeral (messages automatically disappear and a panic wipe with 3 taps), so

most of the data is volatile. The recovered artifacts were almost entirely from the radio buffer and unallocated space. This demonstrates that Bluetooth mesh metadata is more difficult to recover than persistent databases, especially after a device is turned off or the application is wiped. A comparison of Key Findings can be seen in Table 3.

Table 3. Comparison of Key Findings

No	Aspects of Findings	Session	BitChat
1	Amount of Metadata Recovered	47 message metadata	12 hop events
2	Database / Storage	signal.db (SQLCipher)	BLE cache + memory remnants
3	Attachment / File Metadata	Attachment paths + timestamp (full recovery)	Minimal only cache remnants
4	Network / Radio Artifacts	Onion routing hops	RSSI proximity + BLE advertising packets
5	Timestamp & Timeline Quality	High (detailed chronological data)	Medium limited to RSSI and Peer ID
6	Recovery Difficulty	Medium - Hard	Hard
7	Estimation Recovery Rate	65%	25%

3.1.2 Examination

During the inspection phase, an in-depth examination of the images and data acquired during the collection phase was performed using a working copy to maintain the integrity of the original evidence. The process included hash verification, database extraction, file carving in unallocated space and slack space, packet parsing, and system log analysis. In the Session application, the main database file /data/data/network.loki.messenger/databases/signal.db was successfully extracted, containing 47 message metadata records complete with timestamps, Session IDs, thread IDs, and message statuses. Furthermore, metadata attachments and encrypted file paths were successfully recovered using the Scalpel and Foremost tools, and shared preferences and onion routing logs were found in the cache folder. In the BitChat application, the inspection process was more challenging due to its ephemeral nature. Researchers successfully parsed 12 hop events from the remaining BLE packets in the cache and memory, including ephemeral Peer IDs, RSSI values, and advertising packet fragments in the /data/data/com.bitchat/cache/BLE_packets/ folder. Some files in the unallocated space were also successfully recovered, although most of the data was lost due to the panic wipe. This phase produced the artifacts in Table 4, which are structured and ready for further analysis in the next phase.

Table 4. Raw Artifacts Obtained from the Examination

No.	Examination Stages	Session	BitChat	Tools Used
1	Hash Verification	SHA-256 verified	SHA-256 verified	Autopsy, FTK Imager
2	Database Extraction	signal.db → 47 metadata	Cache SQLite & BLE logs	DB Browser for SQLCipher
3	File Carving	Attachment paths & deleted records	Ephemeral cache & unallocated space	Scalpel, Foremost
4	Packet & Log Parsing	Onion routing logs	12 BLE hop events + RSSI	Wireshark, Volatility, nRF Connect
5	Main Results	Rich persistent metadata	Limited volatile radio artifacts	Autopsy + Frida

3.1.3 Analysis

In the analysis phase, all artifacts extracted during the examination were then analyzed in depth to reconstruct the chronology of events, correlate data, establish behavioral patterns, and answer investigative questions (who, what, when, how). The process included creating a super timeline using Plaso/log2timeline, correlating metadata, reconstructing message flows, creating proximity graphs based on RSSI, timing analysis, and detecting communication patterns. In the Session application, a high-quality reconstruction timeline was successfully created. 47 message metadata were correlated with timestamps and onion routing hops, resulting in a clear picture of

the communication chronology along with attachment activities. The correlation between Session IDs and threads also revealed conversation patterns. Meanwhile, in the BitChat application, the analysis focused more on proximity and volatile data; a proximity graph was successfully constructed from 12 hop events along with RSSI values indicating the physical distance between devices, and timing analysis revealed an offline mesh relay pattern. Although the recovery rate was lower (25%), this analysis successfully revealed the characteristics of ephemeral local communication that is difficult to detect using conventional methods. Overall, this phase demonstrates that Session provides richer and more easily reconstructed metadata for forensic timeline purposes, while BitChat provides unique value in physical proximity information, albeit with limitations due to its ephemeral nature. This can be seen more clearly in Table 5.

Table 5. Results Analysis

No.	Analysis Stage	Session	BitChat	Tools
1	Timeline Reconstruction	High quality (47 metadata + timestamp + onion hops)	Medium (12 hop events + timing)	Plaso / log2timeline, Autopsy
2	Metadata Correlation	Session ID ↔ Thread ↔ The attachment has been successfully correlated	Ephemeral Peer ID ↔ RSSI correlation	Autopsy, Python scripting
3	Proximity & Network Graph	The onion routing hops are clearly visible.	Proximity graph derived from RSSI (physical distance).	Wireshark, Gephi
4	Pattern & Behavior Analysis	Conversation patterns and attachment usage	Offline mesh relay pattern	Volatility, Timeline analysis
5	Recovery Rate and Analytical Conclusion	65% – Timeline sangat detail	25% – Proximity information unique	Plaso + Manual correlation

3.1.4 Report

In the Reporting phase, all results from the Collection, Examination, and Analysis phases are presented in a clear, objective, structured, and legally accountable report. This process includes creating an executive summary, compiling key findings and supporting evidence, creating comparison tables, and drawing conclusions and recommendations. All findings are presented without speculation, emphasizing the fact that Session generated 47 messages with rich metadata and a detailed reconstruction timeline at a rate of 65%, while BitChat only generated 12 hop events with unique information but very limited due to its ephemeral nature at a rate of 25%. The final results of this phase can be seen in Table 6. These are comprehensive, repeatable forensic results, ready to be used as evidence in further investigations or research.

Table 6. Results Report

Phase NIST	Session	BitChat	Conclusion
Collection	RAM dump + full filesystem + onion traffic	BLE packets + memory dump before wipe	Volatile data was retrieved first
Examination	47 metadata from signal.db + attachment carving	12 hop events + RSSI parsing	Sessions are richer in persistent artifacts
Analysis	Timeline detail + onion hops correlation (65%)	Proximity graph + timing analysis (25%)	Sessions are superior in timelines, BitChat is superior in proximity
Reporting	A comprehensive report with strong evidence	The report emphasizes the limitations of ephemeral	The difference in metadata durability is very significant.

3.2 Discussion

The forensic simulation results demonstrate that decentralized messaging applications have different levels of metadata recoverability depending on their storage architecture, communication mechanism, and data persistence model. Unlike conventional instant messaging applications such as WhatsApp and Signal, which generally maintain structured local databases

to support message synchronization and user experience, decentralized applications introduce additional challenges because their privacy mechanisms reduce the availability and persistence of forensic artifacts. Previous mobile messaging forensic studies have shown that encrypted messaging applications may still leave recoverable artifacts on mobile devices, including database records, timestamps, application logs, and residual memory data. In this study, Session produced a higher amount of recoverable metadata compared with BitChat. The recovery of 47 metadata records from the SQLCipher database, including timestamps, Session identifiers, thread information, and attachment metadata, indicates that local persistent storage remains a significant source of forensic evidence even when communication content is protected by end-to-end encryption. This finding is consistent with previous forensic investigations of secure messaging applications, where encrypted communication does not necessarily eliminate the existence of local artifacts required for application functionality. Similar approaches have been applied in forensic analysis of applications such as Signal, where investigators focus on extracting application databases, configuration files, and system artifacts rather than attempting to break encryption mechanisms.

However, the forensic characteristics of Session differ from centralized applications such as WhatsApp. In WhatsApp forensic investigations, artifacts are commonly obtained from structured databases such as message stores and application backups, allowing investigators to reconstruct communication timelines with relatively high accuracy. In contrast, Session distributes communication through Oxen onion routing and avoids conventional user identifiers such as phone numbers. As a result, the recovered artifacts provide less direct identity information but still contain valuable metadata for timeline reconstruction and communication pattern analysis. Therefore, Session demonstrates a different forensic challenge: not the absence of artifacts, but the interpretation of decentralized metadata. BitChat presents a different forensic profile because it is designed around ephemeral Bluetooth mesh communication. The recovery of only 12 hop events with RSSI proximity information indicates that most evidence exists temporarily in volatile memory and radio communication buffers. This differs from conventional messaging applications where persistent databases are normally available after device acquisition. The limited recovery rate of BitChat is primarily influenced by its ephemeral design, which reduces long-term artifact retention. From a forensic perspective, this increases the importance of immediate volatile acquisition because delayed acquisition may result in significant evidence loss.

The difference between Session and BitChat reflects a trade-off between application functionality and forensic resilience. Session provides richer persistent artifacts, resulting in better timeline reconstruction capability, while BitChat minimizes artifact persistence and therefore provides stronger resistance against conventional forensic acquisition. This finding supports the principle described in NIST SP 800-86 that forensic investigations depend heavily on identifying appropriate data sources, including files, operating systems, network traffic, and application-generated artifacts. Compared with previous studies focusing mainly on centralized messaging applications such as WhatsApp, Telegram, and Signal, this research extends forensic analysis into decentralized architectures with different evidence-generation mechanisms. The main contribution is not evaluating the cryptographic strength of the applications, but understanding how architectural choices influence metadata exposure and forensic recoverability. The results show that privacy-oriented design does not produce a uniform level of forensic resistance; instead, resilience depends on whether application data is stored persistently or generated temporarily during communication.

4. CONCLUSION

This study evaluated the forensic recoverability and metadata resilience of two decentralized messaging applications, Session and BitChat, using an experimental digital forensic simulation based on the NIST SP 800-86 framework. The investigation focused on the availability, persistence, and recoverability of digital artifacts rather than evaluating the overall security or privacy strength of the applications. The results demonstrate that Session provides a

higher level of forensic recoverability compared with BitChat. Session generated more persistent artifacts, including message metadata, timestamps, Session identifiers, thread information, attachment metadata, and onion routing-related traces extracted from local storage. The availability of these artifacts enabled more detailed timeline reconstruction with an estimated recovery rate of 65%.

In contrast, BitChat demonstrated stronger forensic resilience against conventional acquisition techniques because its communication model relies on ephemeral Bluetooth mesh interactions. The recovered artifacts were mainly obtained from volatile memory and radio communication remnants, including BLE hop events and RSSI proximity information, with a lower estimated recovery rate of 25%. These results indicate that temporary data generation and limited persistent storage significantly reduce the availability of forensic evidence. The findings highlight that decentralized messaging applications produce different forensic challenges depending on their architectural design. Applications with persistent local storage tend to provide richer artifacts for forensic analysis, while ephemeral communication models reduce artifact retention and require faster acquisition of volatile evidence. Therefore, the contribution of this research is the evaluation of metadata exposure and forensic recoverability characteristics in decentralized messaging environments. Future forensic investigations should consider application-specific artifact sources, acquisition timing, and communication architecture when analyzing privacy-oriented messaging applications.

5. FUTURE WORK

This study provides practical implications for digital forensic investigators, application developers, and researchers involved in the analysis of privacy-oriented messaging applications. The findings indicate that forensic acquisition strategies should be adapted to the architectural characteristics of each application. Applications with persistent storage mechanisms, such as Session, require detailed examination of local databases, attachment metadata, and application-generated artifacts, while ephemeral applications such as BitChat require rapid acquisition of volatile memory and radio communication artifacts because relevant evidence may disappear after communication sessions end or deletion mechanisms are activated. For application developers, this research highlights the relationship between application design choices and forensic artifact availability. Reducing unnecessary metadata storage, improving secure deletion mechanisms, and managing temporary communication data effectively can influence artifact persistence and forensic recoverability. Furthermore, forensic tool developers should consider improving acquisition and analysis capabilities for decentralized messaging environments because conventional forensic workflows designed for centralized messaging applications may not fully address onion routing architectures, peer-to-peer communication, or Bluetooth mesh-based systems. Future research should expand this work by evaluating additional decentralized messaging applications with different communication architectures, including federated, peer-to-peer, and mesh-based platforms. Testing across multiple operating systems, such as iOS and desktop environments, as well as conducting experiments under more realistic communication scenarios involving multiple devices, longer interaction periods, and different deletion conditions, may provide a broader understanding of artifact persistence and forensic resilience. Further investigation into memory analysis, network artifact extraction, automated artifact classification, and cross-application correlation techniques is also required to support more effective forensic examination of increasingly complex privacy-focused communication systems.

REFERENCE

[1] A. Apriliani, K. Hijjayanti, And S. Suhairoh, “Analisis Keaslian Citra Dengan Menggunakan Exif Metadata,” *Cess (Journal Of Computer Engineering, System And Science)*, Vol. 5, No. 1, 2020, doi: 10.24114/cess.v5i1.15600.

[2] M. Fransiskus And N. P, "Analisis Digital Forensik Metadata Pada Rekayasa Digital Image Sebagai Barang Bukti Digital," *Jurnal Sains Dan Komputer*, Vol. 8, No. 01, 2024, doi: 10.61179/jurnalinfact.v8i01.439.

[3] K. Eka Purnama, C. Rozikin, And A. Ali Ridha, "Analisis Forensic Citra Digital Menggunakan Teknik Error Level Analysis Dan Metadata Berdasarkan Metode NIST," *Jati (Jurnal Mahasiswa Teknik Informatika)*, Vol. 7, No. 2, 2023, doi: 10.36040/jati.v7i2.6660.

[4] R. Anjelina And N. P, "Analisis Forensik Dengan Menerapkan Metadata Dan Hash Studi Kasus Pada Rekaman Video," *Informatik : Jurnal Ilmu Komputer*, Vol. 20, No. 3, 2024, doi: 10.52958/iftk.v20i3.8770.

[5] H. A. Syuhrawardi, S. Anraeni, And E. I. Alwi, "Analisis Perbandingan Metadata Bukti Digital Gambar Dengan Menggunakan Tools Metadata++," *Linier: Literatur Informatika Dan Komputer*, Vol. 2, No. 1, 2025, doi: 10.33096/linier.v2i1.2782.

[6] N. C. P. Trisuwita And R. P. Kristianto, "Analisis Metadata Exiftool Dan Framework NIST Untuk Deteksi Manipulasi Citra," *Jupiter : Journal Of Computer & Information Technology*, Vol. 6, No. 2, 2025, doi: 10.53990/jupiter.v6i2.462.

[7] I. Riadi, A. Fadlil, And A. Fauzan, "A Study Of Mobile Forensic Tools Evaluation On Android-Based Line Messenger," *International Journal Of Advanced Computer Science And Applications*, Vol. 9, No. 10, 2018, doi: 10.14569/ijacsa.2018.091024.

[8] M. H. A. Husen And F. Firmansyah, "Implementation Of Mikhmon Server For Qos Optimization And Traffic Control On Mikhmon Hotspot Network At Amicom Net," *Mobile And Forensics*, Vol. 7, No. 2, 2025, doi: 10.12928/mf.v7i2.14076.

[9] F. Firmansyah, B. Wibisana, And M. Jordan, "Analyze Threats In A Virtual Lab Network Using Live Forensic Methods On Metarouter," *International Journal Of Engineering And Computer Science Applications (Ijecsa)*, Vol. 4, No. 1, 2025, doi: 10.30812/ijecsa.v4i1.4784.

[10] I. Riadi, A. Yudhana, And G. P. I. Fanani, "Comparative Analysis Of Forensic Software On Android-Based Michat Using Acpo And Dfrws Framework," *Jurnal Resti*, Vol. 7, No. 2, 2023, doi: 10.29207/resti.v7i2.4547.

[11] I. Riadi, Herman, And N. H. Siregar, "Mobile Forensic Analysis Of Signal Messenger Application On Android Using Digital Forensic Research Workshop (Dfrws) Framework," *Ingenierie Des Systemes D'information*, Vol. 27, No. 6, 2022, doi: 10.18280/isi.270606.

[12] I. Riadi, Sunardi, And P. Widiandana, "Cyberbullying Detection On Instant Messaging Services Using Rocchio And Digital Forensics Research Workshop Framework," *Journal Of Engineering Science And Technology*, Vol. 17, No. 2, 2022.

[13] I. Riadi, R. Umar, And M. I. Syahib, "Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute Of Standards And Technology (NIST)," *Jurnal Resti*, Vol. 5, No. 1, 2021, doi: 10.29207/resti.v5i1.2626.

[14] W. Panggah, S. Sunardi, And I. Riadi, "Forensik Digital Cyberbullying Pada Grup Whatsapp Menggunakan National Institute Of Standards And Technology," *Insect (Informatics And Security) : Jurnal Teknik Informatika*, Vol. 12, No. 1, Pp. 34–41, Mar. 2026, doi: https://doi.org/10.33506/insect.v12i01.5275.

[15] Y. Safitri, F. Firmansyah, And M. A. Mu'min, "Mobile Forensic Analysis On Imo Messenger Application Using Acpo And Nij Frameworks," *Insect (Informatics And Security): Jurnal Teknik Informatika*, Vol. 11, No. 1, 2025, doi: 10.33506/insect.v10i2.4052.

[16] F. R. Adriani And I. Riadi, "Forensic Analysis Of Website In Cyberbullying Cases On Instagram Using National Institute Of Justice Method," *Int. J. Comput. Appl.*, Vol. 187, No. 38, 2025, doi: 10.5120/Ijca2025925678.

[17] S. A. Putri And I. Riadi, "Mobile Forensic Analysis Of Michat Application In Human Trafficking Cases Using National Institute Of Justice Method," *Int. J. Comput. Appl.*, Vol. 187, No. 37, 2025, doi: 10.5120/ijca2025925638.

[18] A. N. Mansur And I. Riadi, "Digital Forensic Analysis Of Tiktok Application In Defamation Cases Using Digital Forensics Research Workshop Method," *Int. J. Comput. Appl.*, Vol. 187, No. 47, 2025, doi: 10.5120/ijca2025925795.

[19] N. Anwar And I. Riadi, "Analisis Investigasi Forensik Whatsapp Messanger Smartphone Terhadap Whatsapp Berbasis Web," *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, Vol. 3, No. 1, 2017, doi: 10.26555/jiteki.v3i1.6643.

[20] H. S. Alawi, I. Riadi, And S. Sunardi, "Analisis Forensik Digital Terhadap Kasus Penipuan Pada E-Commerce Menggunakan Metode Acpo," *Jurnal Informatika: Jurnal Pengembangan It*, Vol. 10, No. 3, 2025, doi: 10.30591/jpit.v10i3.8604.

[21] C. Umam, L. B. Handoko, C. A. Sari, E. H. Rachmawanto, And L. A. R. Hakim, "Kombinasi Vigenere Dan Autokey Cipher Dalam Proses Proteksi Sms Berbasis Android," *Prosiding Sains Nasional Dan Teknologi*, Vol. 12, No. 1, 2022, doi: 10.36499/psnst.v12i1.7108.

[22] M. Alda And M. I. Rifki, "Implementasi Metode Triple Des Pada Aplikasi Keamanan Pesan Berbasis Mobile," *Jointecs (Journal Of Information Technology And Computer Science)*, Vol. 7, No. 1, 2022, doi: 10.31328/jointecs.v7i1.3281.

[23] D. Darmansyah And A. Halim Hasugian, "Enkripsi Pesan Chat Menggunakan Algoritma Chacha20 Pada Aplikasi Komunikasi Real-Time," *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, Vol. 10, No. 2, 2025, doi: 10.36341/rabit.v10i2.6220.

[24] R. Herzallah, "Probabilistic Message Passing For Decentralized Control Of Stochastic Complex Systems," *IEEE Access*, Vol. 7, 2019, doi: 10.1109/access.2019.2961165.

[25] K. Takeuchi, "Decentralized Generalized Approximate Message-Passing For Tree-Structured Networks," *IEEE Trans. Inf. Theory*, Vol. 70, No. 10, 2024, doi: 10.1109/tit.2024.3449321.

[26] X. Huang And S. Zhou, "Qmnet: Importance-Aware Message Exchange For Decentralized Multi-Agent Reinforcement Learning," *IEEE Trans. Mob. Comput.*, Vol. 23, No. 5, 2024, doi: 10.1109/tmc.2023.3296726.

[27] S. Evangelatos *Et Al.*, "Adaptive Policy-Oriented Cybersecurity: A Decentralized Framework Using Message Passing Algorithms For Dynamic Threat Mitigation," *IEEE Access*, Vol. 13, 2025, doi: 10.1109/access.2025.3559428.

[28] B. M. Jeong, D. S. Jang, And H. L. Choi, "Decentralized Message Passing Algorithm For Heterogeneous Multi-Depot Vehicle Routing Problems," *Operations Research Perspectives*, Vol. 14, 2025, doi: 10.1016/j.orp.2025.100341.

[29] S. Liu, H. Zhang, And Q. Zou, "Decentralized Channel Estimation For The Uplink Of Grant-Free Massive Machine-Type Communications," *IEEE Transactions On Communications*, Vol. 70, No. 2, 2022, doi: 10.1109/tcomm.2021.3126619.

[30] Q. Xie, P. Zheng, Z. Ding, X. Tan, And B. Hu, "Provable Secure And Lightweight Vehicle Message Broadcasting Authentication Protocol With Privacy Protection For Vanets," *Security And Communication Networks*, Vol. 2022, 2022, doi: 10.1155/2022/3372489.

[31] Z. Zhang, Y. Dong, K. Long, X. Wang, And X. Dai, "Decentralized Baseband Processing With Gaussian Message Passing Detection For Uplink Massive Mu-Mimo Systems," *IEEE Trans. Veh. Technol.*, Vol. 71, No. 2, 2022, doi: 10.1109/tvt.2021.3133111.

[32] S. Sen And H. Artuner, "Emulator Forensics Investigation Model (Efim)," *IEEE Access*, Vol. 13, 2025, doi: 10.1109/access.2025.3585096.

[33] R. Pratiwi, L. C. Utami, R. Bima Sakti, And Triase, "Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher," *Bulletin Of Information Technology (Bit)*, Vol. 3, No. 4, 2022, doi: 10.47065/bit.V3i4.420.

[34] S. N. Nugraha, "Penerapan Algoritma Kriptografi Elgamal Pada Aplikasi Pengamanan Pesan Berbasis Website," *Jurnal Informatika Dan Teknik Elektro Terapan*, Vol. 12, No. 3, 2024, doi: 10.23960/jitet.v12i3.4794.

[35] Shravan Vilas Mate, Utkarsha Anandrao Tembhurkar, Vedant Keshawanad Nikhare, Prof. Vaishali Patil, And Saurabh Baijlal Yelekar, "Secure Messaging Application With Steganography-Based Encryption," *International Journal Of Advanced Research In Science, Communication And Technology*, 2025, doi: 10.48175/ijarsct-29873.

[36] R. Karthikeyan, Mopuru Deepika, Nelamala Yashwanth, Athikayala Pranay Kumar Yadav, And Duvuru Mohith Reddy, "Identifying Drug Traffickers On Encrypted Messaging Apps," *International Journal Of Scientific Research In Computer Science, Engineering And Information Technology*, Vol. 11, No. 2, 2025, doi: 10.32628/cseit25112818.

[37] W. A. Prabowo, F. Mohsen, And S. R. Selamat, "Whatsapp Mobile Applications In The Lens Of Digital Forensics: Deciphering The Msgstore.Db.Crypt14 File," *Journal Of Cyber Security And Mobility*, Vol. 14, No. 4, 2025, doi: 10.13052/jcsm2245-1439.1443.

[38] E. C. T. T. Totnay, M. M. Seran, V. V. Y. Tusala, S. T. Mau, And H. L. To, "Enkripsi End-To-End Pada Aplikasi Whatsapp Menggunakan Metode Aes-256," *Blantika: Multidisciplinary Journal*, Vol. 3, No. 7, 2025, doi: 10.57096/blantika.v3i7.380.

[39] A. Pujol, L. Murphy, And C. Thorpe, "Fedoram: A Federated Oblivious Ram Scheme," *IEEE Access*, Vol. 8, 2020, doi: 10.1109/access.2020.3027516.

[40] W. S. Ong And N. H. Ab Rahman, "A Forensic Analysis Visualization Tool For Mobile Instant Messaging Apps," *International Journal On Information And Communication Technology (Ijoict)*, Vol. 6, No. 2, 2020, doi: 10.21108/ijoict.2020.62.530.

[41] D. Wijnberg And N. A. Le-Khac, "Identifying Interception Possibilities For Whatsapp Communication," *Forensic Science International: Digital Investigation*, Vol. 38, 2021, doi: 10.1016/j.fsidi.2021.301132.

[42] A. Ffaizal And A. Luthfi, "Comparison Study Of NIST Sp 800-86 And Iso/Iec 27037 Standards As A Framework For Digital Forensic Evidence Analysis," *Journal Of Information Systems And Informatics*, Vol. 6, No. 2, 2024, doi: 10.51519/journalisi.v6i2.717.

[43] D. Hariyadi, M. W. Indriyanto, And M. Habibi, "Investigasi Dan Analisis Forensik Digital Pada Percakapan Grup Whatsapp Menggunakan NIST Sp 800-86 Dan Support Vector Machine," *Cyber Security Dan Forensik Digital*, Vol. 3, No. 2, 2020, doi: 10.14421/csecurity.2020.3.2.2193.

[44] K. Kent, S. Chevalier, T. Grance, And H. Dang, "Special Publication 800-86 Guide To Integrating Forensic Techniques Into Incident Response Recommendations Of The National Institute Of Standards And Technology."