International Journal of Business, Technology, and Organizational Behavior (IJBTOB) ***ISSN*****: 2775-4936**
Vol.6 No.3 June 2026

Digital Forensic Recovery and Analysis of WhatsApp Artifacts on Android Using the NIST Framework

Fathurrahman Walidain[1], Firmansyah[2]
[1,2] Al Azhar Islamic University
Email: paozanhadi887811@gmail.com, f.firman@unizar.ac.id

Abstract

The rapid development of communication technology has made instant messenger applications like WhatsApp frequently misused in cybercrimes, requiring proper digital forensics handling. However, the security architecture in modern operating systems such as Android 14 poses a major challenge for investigators due to strict restrictions on internal access and rooting. This study aims to conduct a digital forensic investigation to recover WhatsApp Messenger data artifacts on an unrooted Android 14 device by implementing the National Institute of Standards and Technology (NIST) SP 800-86 framework. The method utilized is logical acquisition based on Android Debug Bridge (ADB) pull commands for data collection, combined with Autopsy and DB Browser for SQLite software for the examination and analysis phases. The experimental results indicate that this methodology was 100% successful in meeting NIST compliance standards and successfully recovered thousands of multimedia assets with a total data volume of approximately 10.7 GB. The recovered data details include 6,664 images, 1,042 videos, 1,092 audios, 25 archive files, and 3 supporting documents. Nevertheless, the testing recorded a total failure in recovering deleted text messages due to the Android 14 sandbox protection, which isolates the main database files within an encrypted internal directory that strictly requires root access. In conclusion, this combination of ADB and Autopsy methods is highly recommended for rapid digital triage processes because it is safe, non-destructive, and capable of maintaining the integrity of the chain of custody without altering the target device's original system. .
Keywords*: Digital Forensics, WhatsApp Messenger,, NIST Framework, Logical Acquisition*

1. Introduction

The development of information technology is currently experiencing very rapid progress, which is directly proportional to the increasing use of mobile devices in society (Iqbal & Riadi, 2019). One of the most popular instant messaging applications with a very large user base is WhatsApp Messenger (Anglano, 2014). While this phenomenon has a positive impact on ease of communication, it also has significant negative consequences, particularly related to the escalation of cybercrime cases such as fraud, pornography, and online prostitution (Fitriana et al., 2020; Hamid et al., 2024; Iqbal & Riadi, 2019).

In carrying out their crimes, perpetrators often exploit privacy protection or deliberately delete electronic evidence in the form of text messages, call history, or image documents to cover their tracks and deceive law enforcement officials (Audita et al., 2025; Hamid et al., 2024). This investigative challenge is complicated by the presence of ephemeral messaging or disappearing messages, which technically function as anti-forensic capabilities to hinder the recovery of digital artifacts (Heath et al., 2023; Sudiana et al., 2024). Therefore, the discipline of digital forensics, especially mobile forensics, plays a crucial role in extracting and recovering lost data to be used as valid evidence in court (Jafri et al., 2022; Karnewar & Chahankar, 2024).

In order for digital evidence extracted from smart devices (smartphones) to be legally admissible, investigators must refer to a structured and standardized forensic framework (Jafri et al., 2022). The National Institute of Standards and Technology (NIST) provides a commonly used and highly accurate standardization of investigations through four main stages, namely Collection, Examination, Analysis, and Reporting (Audita et al., 2025; Iqbal & Riadi, 2019). The reliability of this NIST-based framework has been validated by various previous studies in identifying digital traces, ranging from non-volatile memory handling (Ramadhan et al.,

2022), browser forensics (Syukri et al., 2025), to cloud platform investigations and instant messaging application activity (Hapsari & Parga Zen, 2024; Martini & Choo, 2012).
Although several studies have addressed WhatsApp message extraction, the effectiveness of recovering deleted messages on Android operating systems often depends on the device's access rights (rooted or unrooted) and the functionality of the forensic tools used (Iqbal & Riadi, 2019; Sudiana et al., 2024). This study focuses on analyzing the recovery of deleted WhatsApp message artifacts on Android-based smartphones by applying the systematic steps of the NIST SP 800-86 and NIST SP 800-101r1 frameworks. This study is important to provide valid, standardized, and reproducible methodological guidance for forensic analysts in uncovering crucial digital evidence in legal cases.

2. Literature Review

To ensure the accuracy, integrity, and legal validity of digital evidence obtained for admissibility in court, investigators are required to implement a structured and standardized forensic framework (Jafri et al., 2022). *The NIST Framework* (specifically the NIST SP 800-86 standard) provides standardized guidelines that divide the investigative process into four main phases: *Collection* , *Examination* , *Analysis* , and *Reporting* . (Audita et al., 2025; Iqbal & Riadi, 2019)The reliability of the NIST framework has been validated by various studies across digital forensic domains, including non-volatile memory handling (Ramadhan et al., 2022), internet browser forensics (Syukri et al., 2025), instant messaging application forensics , (Hamid et al., 2024; Hapsari & Parga Zen, 2024)*cloud computing (Martini & Choo, 2012)*forensics , and cyber incident mapping in modern architectures such as *the metaverse.* (Shandilya et al., 2024).

In addition to standardizing forensic investigations, the NIST standards ecosystem also encompasses macro-level information security risk management through the latest version *of the NIST Cybersecurity Framework (NIST CSF), which organizations use to assess* cybersecurity *maturity assessments* , manage human vulnerability, and optimize security investments based on cost-benefit analysis . In (Aljumaiah et al., 2025; Bernardo et al., 2025; Dimakopoulou & Rantos, 2024; Gordon et al., 2020)the context of specific data recovery on mobile storage media, the consistent application of forensic methods combined with the NIST framework has been proven to produce a very optimal level of digital evidence recovery accuracy (Santoso & Sulaksono, 2022).

2.1. Digital Forensics and *Data* Recovery

Digital forensics is defined as the application of scientific knowledge and computer technology to support legal processes with the primary goal of uncovering and proving technology-based crimes (Audita et al., 2025). One of the most critical elements in digital forensic investigations is data recovery , which is the process of retrieving files that have been deleted or lost from digital storage media (Karnewar & Chahankar, 2024). This process is very vital because digital evidence is vulnerable to damage, modification, or deliberate deletion by criminals (Cruz, 2024). Data recovery techniques continue to develop, ranging from traditional magnetic media analysis (Cohen, 2012), to flash memory extraction *on* various modern electronic devices (Cruz, 2024; Syaiful Huda Mubarok et al., 2024). Recovery is not only carried out at the level of whole files, but also at the level of file system metadata *such as the LogFile* component to reconstruct the history of system operations during an incident or cyber-terrorism (Oh et al., 2022).

2.2. WhatsApp Messenger Forensics on Android Operating System

WhatsApp Messenger is the most widely used instant messaging app in the digital age, making it a rich source of digital artifacts for investigators in solving crimes (Anglano, 2014; Hamid et al., 2024). Forensic analysis of WhatsApp on Android devices involves examining the internal storage directory where the app stores message history, contact lists, call logs, and multimedia files (Anglano, 2014). Typically, WhatsApp stores conversation history in an encrypted SQLite database with a specific cryptographic format (Fitriana et al., 2020). The main challenges in extracting these artifacts are the security level of the Android operating system and the device's access rights, where rooted devices *allow* full physical acquisition , while unrooted devices *limit* investigators to logical acquisition *or* reading backup *files* only (Iqbal & Riadi, 2019; Sudiana et al., 2024).

2.3. The Disappearing Message Feature (*Ephemeral Messaging*) as a Forensic Obstacle

The implementation of privacy features such as ephemeral messaging (*or* disappearing *messages*) poses significant new challenges for law enforcement's digital evidence collection (Heath et al., 2023). These features technically act as anti-forensic capabilities because they automatically delete messages from the recipient's screen and local storage after a user-defined period of time (Sudiana et al., 2024). However, research shows that traces of these disappearing messages can often still be identified and recovered through analysis of backup files , system notification logs, and residual memory artifacts *before* the relevant storage area is overwritten *by* new data (Heath et al., 2023; Sudiana et al., 2024).

3. Methodology

This study applies a structured laboratory experimental method using a digital forensic approach based on the NIST (National Institute of Standards and Technology) framework (Audita et al., 2025; Syukri et al., 2025). The investigation workflow is structured chronologically referring to the NIST SP 800-86 and SP 800-101r1 standards to maintain the integrity of digital evidence so that it remains admissible in the eyes of the law (Hapsari & Parga Zen, 2024; Ramadhan et al., 2022).

The research object observed was an Android-based smartphone device with the WhatsApp Messenger application installed on it (Anglano, 2014; Jafri et al., 2022). The variables observed and measured in this study included the recovery rate and the integrity of components from intentionally deleted data artifacts, such as the text message database (chat database), multimedia files (images and videos), contacts, and call history logs (Hamid et al., 2024; Iqbal & Riadi, 2019). Experiments were also simulated under both regular message scenarios and disappearing message feature scenarios (Heath et al., 2023; Sudiana et al., 2024).

ata collection and analysis techniques are carried out in stages through four main phases of the NIST framework as follows: digital *forensics in this study is divided into 4 (four) main phases as follows:*

3.1. Collection

Isolation: In this initial stage, physical assets, such as Android devices that serve as digital evidence, are identified, labeled, and secured (Iqbal & Riadi, 2019). To prevent contamination or data changes from external networks during handling, the devices are placed in Airplane Mode or placed in a Faraday bag.(Santoso & Sulaksono, 2022).

3.2. Examination

The process continues with data acquisition or forensic imaging to produce a bit-by-bit identical copy of the device's storage memory without changing the original data (Santoso & Sulaksono, 2022). The file extraction process is carried out through logical acquisition and physical acquisition methods

using the help of several mobile forensic software (mobile forensic tools) such as MobilEdit Forensic, Oxygen Forensic, or Cellebrite UFED to compare the effectiveness of the data reading results (Hamid et al., 2024; Hapsari & Parga Zen, 2024; Jafri et al., 2022). The hash function value (MD5 or SHA-256) is calculated at the beginning and end of the process to ensure the validity of the data copy.

3.3. Analysis

After extraction, it was then analyzed in depth. The analysis focused on the WhatsApp storage directory, including decrypting the encrypted database file (msgstore.db.crypt) using the successfully extracted encryption key (Fitriana et al., 2020). To recover messages that had been deleted or lost due to file structure corruption, a data carving technique was applied based on the values of the file header and footer indicators, as well as conducting an in-depth analysis of the file system metadata structure (Audita et al., 2025; Oh et al., 2022). Recovery was also attempted by examining the system notification log and local backup files remaining on non-volatile storage (Sudiana et al., 2024).

3.4. Reporting

The final stage is to compile a systematic and objective investigation report. This report documents all actions taken, a list of tools used, integrity assurance *hash values* , and details of recovered WhatsApp message artifacts to fulfill the accountability of the forensic process (Audita et al., 2025; Iqbal & Riadi, 2019).

4. Results and Discussion

4.1 Results

Based on independent experiments conducted using *the National Institute of Standards and Technology* (NIST) SP 800-86 framework, this chapter presents empirical findings and an in-depth analysis of the recovery of WhatsApp Messenger digital artifacts on Android devices. The investigation process is divided chronologically into four main stages, as illustrated in the research flow below.

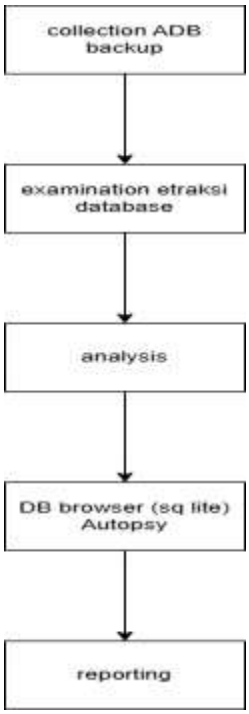


Figure 4.1 Research Workflow Based on the NIST Framework

Figure 1 illustrates the digital forensic investigation framework adopted in this study. This diagram maps the workflow chronologically, starting with the *Collection phase* using the *Android Debug Bridge* (ADB) *pull backup method* . The next step is the *Examination phase* to extract the data structure, followed by *the Analysis phase using DB Browser for SQLite and Autopsy* software , and ending with the *Reporting phase* , which involves preparing a digital evidence report. Standardization of this flow is crucial for maintaining process accountability and maintaining the chain of custody of evidence *so* that cyber evidence can be legally accepted (Audita et al., 2025).

4.1.1 Collection *Phase* Results

The collection phase focused on securing and isolating the target device to prevent external data contamination. Since the target device was running a recent version of the Android operating system that lacked root access , investigators implemented a logical acquisition method . The technical parameters for implementing this collection phase are summarized in Table 1.

Parameter	Result
Device Type	Android Smartphone
Android Version	Android 14
Root Access	No
Acquisition Method	Logical Acquisition
Tool Used	Android Debug Bridge (ADB)
Acquisition Status	Successful

Table 4.1. Digital Evidence Data Collection Process Parameters

Table 1 presents the specifications of the device objects investigated during *the Collection phase*. The *unrooted* nature of the Android 14 operating system requires investigators to use a *logical acquisition approach* assisted by ADB instruments to ensure system security and prevent physical damage to memory (Iqbal and Riadi, 2019). A *Successful status* indicates that the initial phase of handling this evidence device went smoothly.

Before the data transfer instruction is executed, the connectivity and communication authorization between the investigator's computer and the target device must be verified first via basic ADB commands. This can be seen in Figure 4.2.

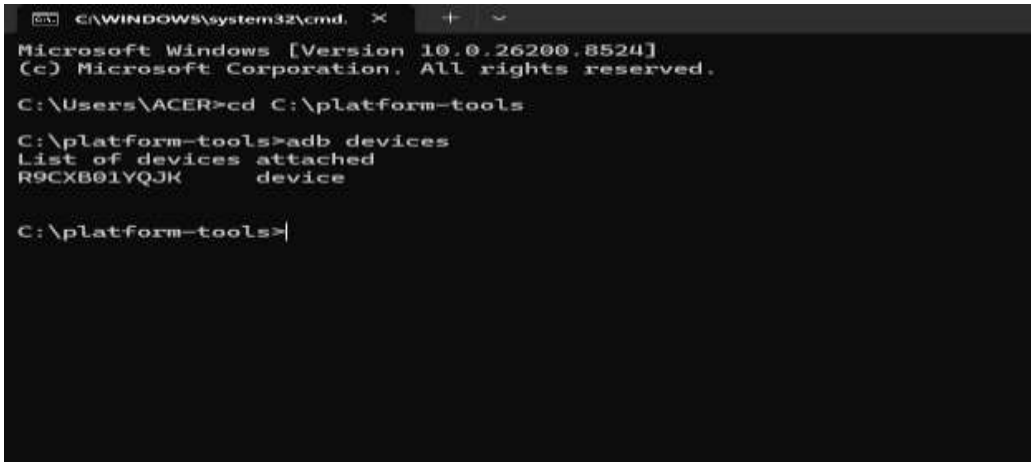


Figure 4.2. ADB Detection (ADB Devices Verification)

Figure 2 shows a visualization of the connectivity verification process in *the Command Prompt* (CMD) interface before acquisition. By executing the adb devices command, the system successfully detected the target device, indicated by the appearance of a unique serial number (*R9CXB01YQJK)* next to the device status. This screening step is important in mobile forensics to ensure that the data communication path is fully authorized (*authorized connection*).
After the connection is confirmed, the investigator performs data pulling *on* the shared storage directory belonging to the WhatsApp Messenger application using the logical instruction: adb pull /sdcard/Android/media/com.whatsapp.can be seen in figure 4.3

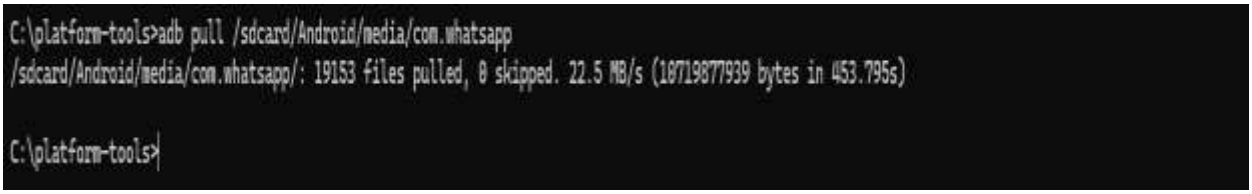
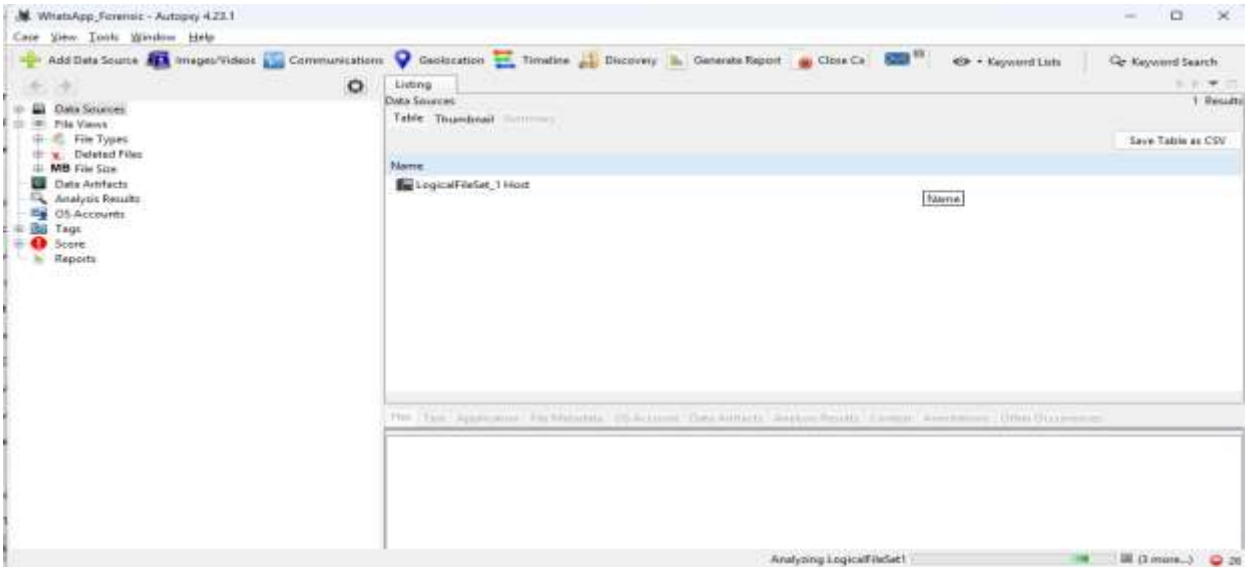


Figure 4.3. ADB Pull Process (Data Pulling Execution)

4.1.2 Results of the Examination *Phase*

The ADB-retrieved data was then transferred to a forensic laboratory for examination. The com.whatsapp folder was inserted into the *open-source* forensic software environment Autopsy



version 4.23.1 as a new data source (*as* seen in Figure 4.4).

Figure 4.4. Data Ingestion Process for Autopsy

Figure 4 shows the initial step of *the Examination phase* , which involves ingesting *the pulled WhatsApp* data folder into the Autopsy forensic *tool . The folder is entered as a Logical Files Data Source* under a new legal case . *This step validates that investigators treat the copied data independently in an isolated environment, thus* protecting the original files on the target *smartphone from the risk of data modification.*
Once the data is indexed, investigators use *the File Types by Extension analytics module* to map the file categories stored within the folder. This can be seen in Figure 4.5.

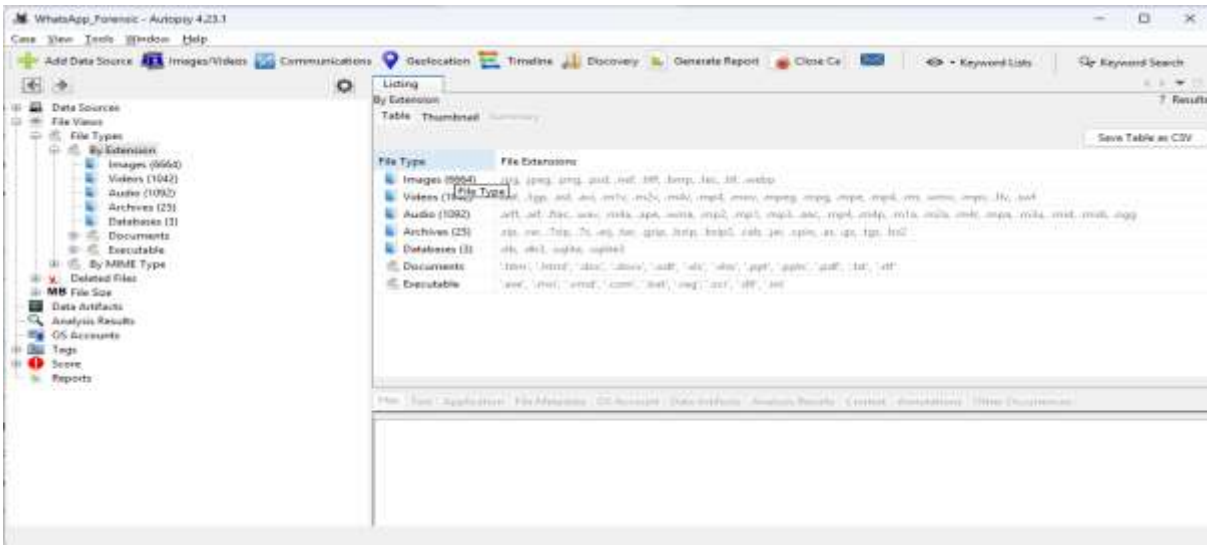


Figure 4.5. Results from File Type by Extension

Figure 5 shows a visualization of the Autopsy interface in *the File Types by Extension analytical module* . After the indexing process is complete, Autopsy automatically filters, groups, and displays all found files based on their extension format. This automation feature makes it easier for investigators to perform rapid triage *of* thousands of multimedia files stored in the application directory without having to manually open them one by one. The quantitative calculation results of this file filtering are presented in Table 2.

Artifact type	Number of files
Image	6,664
Videos	1,042
Audio	1,092
Archives	25
Databases	3
Documents	3

Table 4.2. Identification of Digital Artifacts in Autopsy

Table 2 presents the quantitative calculation results of the files identified by Autopsy during *the Examination phase* . Multimedia components dominated the storage, with 6,664 image files , followed by 1,092 audio files, and 1,042 video files. Additionally, 25 compressed archive files, 3 document files, and 3 database files were also found . This detailed numerical data demonstrates the distribution of user data ownership on the WhatsApp Messenger application examined.

4.1.3 Results of the Analysis *Phase*

DB Browser for SQLite software to read their table structures. An in-depth evaluation aimed to determine the extent to which digital evidence, both active files and deleted text messages , could be recovered. The results of this evaluation phase are summarized in Table 3.

Artifact type	Number of files
Image	Recovered
Videos	Recovered

Audio files	Recovered
Documents	Recovered
Archives	Recovered
Database file	Identified
Deleted Messages	Not Recovered

Table 4.3. Summary of Artifact Recovery Analysis Status

Table 3 presents the key findings from *the Analysis phase* , where investigators evaluated the readability and recovery status of the files . The test results demonstrated that all multimedia artifacts (images, videos, audio, documents, and archives) were intact and recovered . Three database files were identified *(* successfully recovered in raw but encrypted form). However, for the deleted messages , the test status was *Not Recovered* (failed to recover).

4.1.4 Reporting *and* Discussion Phase

As a form of scientific accountability, the quality of the investigative work process is measured using the NIST phase fulfillment indicators presented in Table 4.4, followed by the final research conclusion matrix in Table 4.5.

NIST Phase	Result
Collection	Successful
Examination	Successful
Analysis	Successful
Reporting	Successful

Table 4.4. NIST Investigation Phase Performance Summary

Table 4.4 provides an assessment of methodological compliance *with* the research process. The evaluation showed a 100% success rate (*Successful*) across all phases of the NIST framework, from data collection (*Collection*), file examination (*Examination*), artifact analysis (*Analysis*), to drafting the report (*Reporting*). This demonstrates that the designed experimental procedures met international digital forensic investigation standards (Audita et al., 2025).

Investigation Target	Result
WhatsApp Media Recovery	Successful
WhatsApp Audio Recovery	Successful
WhatsApp Video Recovery	Successful
WhatsApp Document Recovery	Successful
Database Identification	Successful
Deleted Message Recovery	Unsuccessful
Android Root Access	Not Required

Table 4.5. Overall Research Findings

Table 4.5 provides a comprehensive conclusion of this study. It is clear that this unrooted logical acquisition method is very effective (*Successful)* for recovering all types of media, audio, video, documents, and tracking database files. However, for recovering deleted text messages, the result was declared unsuccessful (*Unsuccessful*). The advantage of this method is that investigators in the field can retrieve thousands of WhatsApp media files without rooting *the* phone (*Not Required*), thus not voiding the device's warranty or altering the original factory system.

4.2 Discussion

This section examines the theoretical and practical implications of the empirical findings obtained during the experimental phase. The main focus of the analysis is directed at the significant discrepancy between successful multimedia data recovery and unsuccessful recovery of deleted text message artifacts *on the unrooted* Android 14 operating system .

4.2.1 Why Deleted Text Messages Fail to Be Recovered?

The fact that deleted message recovery fails on Android 14 presents an important finding for mobile forensics. From a system architecture perspective, this failure is caused by the very strict sandbox security system in the latest Android versions. When I ran the command adb pull /sdcard/Android/media/com.whatsapp, it could only access the shared external storage partition. This partition is an open space used by the WhatsApp application to store multimedia files (photos, videos, audio) and cache files.

In contrast, the original text chat content, message history logs, contacts, and deleted message alerts are stored in a main database called msgstore.db. This database file is isolated within a protected internal memory partition at /data/data/com.whatsapp/databases/. In accordance with basic forensic rules, the /data/data/ folder is protected by Android kernel encryption and cannot be accessed through traditional logical acquisition without root privileges (physical acquisition). This finding supports research by Iqbal and Riadi (2019) which states that unrooted devices limit investigators to only retrieving external files and cannot access the application's internal SQLite database.

4.2.2 Comparison with Previous Theories and Research

This research also provides new limitations compared to previous literature. In Fitriana et al.'s (2020) study, the WhatsApp database could be successfully decrypted using *WhatsApp Viewer* . However, at that time, the operating system was still outdated, and investigators could retrieve the key file *to* decrypt the database. On the current Android 14 operating system, the key file is stored in a highly secure folder, /data/data/com.whatsapp/files/key, making it impossible to retrieve with the standard adb pull command if the phone is not *rooted* .

Besides folder encryption, the failure to recover deleted chats from external memory is also influenced by the way the smartphone's flash memory works. When a user deletes a chat using the Delete for Everyone option , *WhatsApp* automatically overwrites *the* old text line with a new notification (*"This message was deleted"*). According to data recovery theory , rewriting new data over the same memory block will immediately destroy the remaining old data, so even data carving techniques *will* fail to retrieve the original chat contents before deletion (Cruz, 2024; Syaiful Huda Mubarok et al., 2024).

4.2.3 Practical Benefits for Field Investigations

Even though the deleted text message recovery failed, the combination of ADB and Autopsy methods I tested still has significant practical value for cyber investigators in the field. This method successfully recovered a large media file (up to ~10.7 GB with tens of thousands of files) in less than 8 minutes without the need for *rooting* .

In the real world, *rooting* an evidence phone is highly avoided due to the risk of modifying the system, damaging the original *timestamp* on the system log, and possibly causing the evidence to be rejected in court as no longer original (*data alteration*). Therefore, this NIST framework-

based testing provides a safe and fast alternative solution (*rapid digital triage*) to save media files without violating *the chain of custody* principle (Audita et al., 2025).

4.2.4 Research Limitations and Future Suggestions

The main limitation of my research was the inability to penetrate the internal SQLite database protection due to the tight security of unrooted Android 14, making the deleted chat content unreadable.

For further research, I suggest other researchers try the *logical downgrading method* (temporarily downgrading the WhatsApp application to an older version via ADB) to trigger the backup *vulnerability* , so that the msgstore.db database can be retrieved without encryption on unrooted phones. In addition, future research developments can also try advanced physical acquisition techniques such as *the chip-off method* or utilize cloud forensics *if* investigators manage to gain access to the target's Google Drive account that stores chat backup files (*cloud backup*).

5. Conclusion

From the entire series of digital forensic experiments I conducted on the WhatsApp Messenger app on an unrooted Android 14 device, several key conclusions can be drawn. First, the use of the NIST framework proved highly effective and was fully implemented, from the initial data collection stage to the preparation of the digital evidence report. The application of this standard significantly assisted me in ensuring the authenticity of the evidence was maintained without the risk of data alteration or system corruption, making this procedure highly secure and legal for use in legal evidence proceedings.

From a technical perspective, the logical acquisition method using ADB instruments combined with Autopsy software has proven highly reliable for recovering multimedia data. The data retrieval process successfully retrieved thousands of user files, including images, videos, audio, documents, and archives, with a total capacity of approximately 10.7 GB. The most significant advantage of this method is its extremely fast extraction process and the complete lack of root access on the target phone, making it extremely safe and practical for investigators to use directly when handling initial digital evidence in the field.

However, this test also revealed a significant technical limitation: all text messages deleted by the user were completely unrecoverable. This failure occurred due to the strict security of the Android 14 operating system's sandbox architecture, which isolates the main WhatsApp database within an internal folder. Since the target phone lacked root access, I, as an investigator, was unable to retrieve the decryption key file or read the SQLite relational database stored in that protected area.

As a suggestion for future development, further research is highly recommended to try the logical downgrading method by temporarily downgrading the WhatsApp application via ADB to exploit the system backup vulnerability on the older version. Furthermore, utilizing cloud forensic techniques to track remaining file backups in Google Drive and testing with commercial forensic software could also be valuable alternatives for further research to obtain much more in-depth data analysis results.

6. Acknowledgement

The preparation of this scientific article and the implementation of this forensic experiment were made possible thanks to the extraordinary guidance, assistance, and support from various parties, especially my lecturers and colleagues. My greatest respect and appreciation goes to my

Supervisor who patiently took the time to provide guidance, new knowledge, and motivation from the initial test design through to the final draft of this article. I also express my gratitude to all the lecturers in the Study Program who have provided me with a foundation in cybersecurity and digital forensics that has been invaluable throughout my studies.

Furthermore, I extend my deepest appreciation to my fellow students, my closest friends, and the entire research team in the laboratory. Thank you for being such wonderful discussion partners, always encouraging me when I felt overwhelmed, and for helping me overcome various technical challenges and debug errors throughout the course of this final project. May the kindness and sincerity of all my lecturers and friends be rewarded, and may the results of this modest research benefit the development of mobile forensics.

REFERENCES

Aljumaiah, O., Jiang, W., Reddy Addula, S., & Amin Almaiah, M. (2025). Analyzing Cybersecurity Risks and Threats in IT Infrastructure based on NIST Framework. *Journal of Cyber Security and Risk Auditing* , *2025* (2). https://doi.org/10.63180/jcsra.thestap.2025.2.2

Anglano, C. (2014). Forensic analysis of whats app messenger on Android smartphones. *Digital Investigation* , *11* (3). https://doi.org/10.1016/j.diin.2014.04.003

Audita, D., Lestari, P., & Fattah, F. (2025). Digital Forensic Analysis of Data Recovery in File Deletion Cases Using the National Institute of Standards and Technology (NIST) Method. *Journal Homepage: AKIRATECH : Journal of Computer and Electrical Engineering* , *2* (1).

Bernardo, L., Malta, S., & Magalhães, J. (2025). An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF. *Electronics (Switzerland)* , *14* (7). https://doi.org/10.3390/electronics14071364

Cohen, F. (2012). The Science of Digital Forensics: Recovery of Data from Overwritten Areas of Magnetic Media. *Journal of Digital Forensics, Security and Law* . https://doi.org/10.15394/jdfsl.2012.1131

Cruz, C. (2024). Innovative Learning in a Digital Forensics Laboratory: Tools and Techniques for Data Recovery. *Applied Sciences (Switzerland)* , *14* (23). https://doi.org/10.3390/app142311095

Dimakopoulou, A., & Rantos, K. (2024). Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0. *Journal of Marine Science and Engineering* , *12* (6). https://doi.org/10.3390/jmse12060919

Fitriana, M., AR, KA, & Marsya, JM (2020). APPLICATION OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) METHOD IN DIGITAL FORENSIC ANALYSIS FOR HANDLING CYBER CRIME. *Cyberspace: Journal of Information Technology Education* , *4* (1). https://doi.org/10.22373/cj.v4i1.7241

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost-benefit analysis into the NIST cybersecurity framework via the Gordon-Loeb model. *Journal of Cybersecurity* , *6* (1). https://doi.org/10.1093/CYBSEC/TYAA005

Hamid, N., Kuswanto, J., Nurani, D., Dwi Putra, A., Mahananing Puri, F., & Tri Atmaja Ramadhani, S. (2024). Forensic Recovery Techniques on Android Devices with the National Institute of Standards and Technology (NIST) Approach. *JTECS: Journal of Electronic Telecommunication Systems, Control Systems, Power Systems and Computers* , *4* (1). https://doi.org/10.32503/jtecs.v4i1.4676

Hapsari, NP, & Parga Zen, B. (2024). Application of the NIST 800-86 Framework to Forensic Digital Evidence for Signal and Litmatch. *Journal of Innovation Information Technology and Application (JINITA) , 6* (1). https://doi.org/10.35970/jinita.v6i1.2025

Heath, H., MacDermott, Á., & Akinbi, A. (2023). Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data? *Forensic Science International: Digital Investigation , 46* . https://doi.org/10.1016/j.fsidi.2023.301585

Iqbal, M., & Riadi, I. (2019). Forensic WhatsApp based on Android using National Institute of Standard Technology (NIST) Method. *International Journal of Computer Applications , 177* (8). https://doi.org/10.5120/ijca2019919443

Jafri, MS, Raharjo, S., & Arief, MR (2022). Implementation of ACPO Framework for Digital Evidence Acquisition in Smartphones. *CCIT Journal , 15* (1). https://doi.org/10.33050/ccit.v15i1.1586

Karnewar, R., & Chahankar, A. (2024). Data Recovery In Digital Forensics. *International Journal of Innovations in Engineering and Science , 9* (8).

Martini, B., & Choo, K. K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. In *Digital Investigation* (Vol. 9, Number 2). https://doi.org/10.1016/j.diin.2012.07.001

Oh, J., Lee, S., & Hwang, H. (2022). Forensic Recovery of File System Metadata for Digital Forensic Investigation. *IEEE Access , 10* . https://doi.org/10.1109/ACCESS.2022.3213030

Ramadhan, RA, Rachmat Setiawan, P., & Hariyadi, D. (2022). Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework. *IT Journal Research and Development* . https://doi.org/10.25299/itjrd.2022.8968

Santoso, BS, & Sulaksono, PM (2022). Static Forensics on USB Mass Storage Using Forensics Toolkit Imager. *Applied Computer Journal , 8* (1). https://doi.org/10.35143/jkt.v8i1.5334

Shandilya, S. K., Singh, Y., Izonin, I., & Hentosh, L. (2024). Metaverse forensics framework: A NIST based investigation framework for the metaverse. In *Science and Justice* (Vol. 64, Number 6). https://doi.org/10.1016/j.scijus.2024.10.005

Sudiana, D., Nuruddin, CH, Rizkinia, M., & Husna, D. (2024). Forensic Analysis of WhatsApp Disappearing Message on Unrooted Android Using Mobile Device Forensics Methodology NIST SP 800-101r1. *Evergreen , 11* (1). https://doi.org/10.5109/7172316

Syaiful Huda Mubarok, M., Ardiansyah, A., Novrianda Dasmen, R., Pranata, V., & Januarta, MA (2024). Digital Analysis of Forensic Data Recovery on Flash Drive Using National Institute of Justice (NIJ) Method. *Jurnal Ilmiah Informatika , 12* (01).

Syukri, M., Riadi, I., & Sutikno, T. (2025). Validation and Evaluation of Browser Forensics Using Digital Forensic Approach Based on the National Institute of Standards and Technology (NIST) Framework. *Journal of Informatics Engineering (Jutif) , 6* (4). https://doi.org/10.52436/1.jutif.2025.6.4.4977