Forensic Analysis of WhatsApp Disappearing Message on Unrooted Android Using Mobile Device Forensics Methodology NIST SP 800-101r1

Sudiana, Dodi
Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia

Chandra Halim Nuruddin
Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia

Rizkinia, Mia
Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia

Husna, Diyanatul
Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia

https://doi.org/10.5109/7172316

出版情報：Evergreen. 11 (1), pp.516-524, 2024-03. 九州大学グリーンテクノロジー研究教育センター
バージョン：

Forensic Analysis of WhatsApp Disappearing Message on Unrooted Android Using Mobile Device Forensics Methodology NIST SP 800-101r1

Dodi Sudiana[1,2*], Chandra Halim Nuruddin[1], Mia Rizkinia[1,2], Diyanatul Husna[1]

[1]Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Indonesia
[2]Artificial Intelligence and Data Engineering Research Center (AIDE-RC), Faculty of Engineering, Universitas Indonesia, Indonesia

*Author to whom correspondence should be addressed:
E-mail: dodi.sudiana@ui.ac.id

(Received October 22, 2023; Revised January 31, 2024; Accepted March 05, 2024).

Abstract: Digital forensics has a pivotal role in advancing Sustainable Development Goals (SDGs) by enhancing accountability, ensuring digital security, and contributing to environmental sustainability. Digital forensics facilitates investigations for justice, strengthens cybersecurity for resilient infrastructure, and supports environmental sustainability by analyzing data and investigating environmental crimes. WhatsApp's disappearing messages feature, which enables messages to disappear after a user-defined duration, poses new challenges in digital forensics. Criminals can potentially abuse this feature to eliminate message evidence. This research proposes a novel approach to obtaining digital evidence from WhatsApp's disappearing messages using the NIST SP 800-101r1 method. Six scenarios are simulated: forwarded messages, quoted messages, media messages, offline recipients, call history, and unread messages. Forensic analysis of six scenarios from 11–14 June 2023 reveals that 83.33% of disappeared messages could be recovered from backup files and notification logs, while the rest could not be recovered due to missing backup files.

Keywords: disappearing message; forensic analysis; NIST SP 800-101r1; unrooted Android; WhatsApp

1. Introduction

The pivotal role of digital forensics in advancing Sustainable Development Goals (SDGs) focused on Goal 16; digital forensics facilitates investigations, ensuring accountability and transparency. It contributes to Goal 9 by enhancing digital security, mitigating risks, and supporting resilient infrastructure. In alignment with Goal 13, digital forensics investigates environmental crimes and aids data analysis for sustainability[1)]. It is crucial for achieving a just, secure, and sustainable global society. Mobile devices and broadband internet are now essential for daily life and notably impact Indonesia's economy. While the country ranked third in 2016 for peak internet speeds, its average connection speed is significantly lower than South Korea's. However, continuous improvements and government initiatives to connect 57 cities are expected to increase internet penetration[2)]. A recent report by DataReportal states that almost all internet users in Indonesia (99.5%) own a mobile device, and the majority (98.3%) use it to access the internet[3)].

The widespread use of mobile devices has become a key factor in digital forensics, which is now called mobile device forensics (MF), due to the increased proliferation of mobile-based services with new requirements and needs[4)]. Bangladesh's financial sector has witnessed a digital revolution by adopting fintech and mobile banking. Although this transformation poses major challenges to the survival of small microfinance institutions (MFIs) operating in the industry, a potential solution remains to consolidate the financial activities of small MFIs through mergers[5)]. This strategy is intended to address the threats posed by mobile banking and fintech, allowing smaller MFIs to remain competitive and relevant in an increasingly digital financial landscape.

The impact of this digital transformation is not limited to the financial sector. During the COVID-19 pandemic, learning and work activities shifted to online platforms[6)], and most classrooms and workspaces moved to chat rooms. WhatsApp has become the most popular and frequently used social media platform available on mobile devices in Indonesia[7)]. Indonesians spend an average of 29 hours monthly on WhatsApp. These statistics highlight the substantial amount of Indonesian user data stored on

mobile devices in WhatsApp.

Due to WhatsApp's position as the most widely used social media app in Indonesia, data from the app have been used as digital evidence to aid law enforcement processes[8]. This digital evidence can be obtained from chat screenshots, chat exports, or digital forensics. For instance, in the case of drug trafficking involving the former West Sumatra police chief, chat screenshots were presented in court to prove the parties' involvement[9–11]. Obtaining chat screenshots and exports is easier than conducting digital forensics. However, this approach is susceptible to chat manipulation, as Roman Zaikin and Oded Vanunu demonstrated at Black Hat USA 2019[12]. Therefore, digital forensics is advised when there is a need to comply with Indonesian Law Number 11 of 2008 regarding Information and Electronic Transactions[13].

Due to increasing security and privacy concerns on technology usage, various techniques have been developed to improve data security. Sumathi et al. propose a hybrid cryptographic approach using artificial intelligence (AI) and the Internet of Things (IoT) that fills the lack of a well-known traditional cryptographic method[14]. Gera et al. proposed bit-cycling encryption and bi-LSB techniques to show how audio steganography may be used to hide encrypted text[15]. Shaiden et al. proposed a fusion of two algorithms (LSB and PSNR) to hide information inside a cover image that could be implemented effectively on social media platforms such as WhatsApp[16]. Wijnberg introduced a real-time forensic technique for analyzing WhatsApp communication using wiretapping, decryption, open-source intelligence, and WhatsApp Web analysis[17]. Salem et al. conducted experiments on MS Windows systems, finding WhatsApp data in both volatile and non-volatile memories[20]. Alief et al. studied Autopsy's effectiveness in examining WhatsApp's message recall feature on rooted Android[21]. Sengupta et al. introduced a reliable method for extracting WhatsApp data from any mobile device, emphasizing efficiency through advanced tech and practical insights and comparing its effectiveness with traditional methods[22]. Hermawan et al. compared UFED Cellebrite and MOBILedit for analyzing unsent messages on Android social media apps, including WhatsApp[23]. UFED successfully retrieved deleted data, while MOBILedit's encrypted database required root access for analysis. Utomo et al. proposed a forensic analysis of artifacts within the WhatsApp browser to extract data related to conversation sessions, audio files, contact numbers, photos, and videos[24]. Salamh et al. analyzed deleted WhatsApp messages that were never sent, employing manual carving and Magnet ACQUIRE for data extraction from Android devices[25]. Fayyad-Kazan et al. extracted an unencrypted database and encryption key from WhatsApp SQLite Databases on unrooted Android devices using the APK downgrading method and WhatsApp Key Database Extractor tool, successfully reconstructing message history[26]. Shadeed et al. conducted a study to analyze encrypted WhatsApp data on unrooted Android devices[27]. The data was acquired through ADB, utilizing APK downgrading to extract the encryption key, allowing for the decryption of the message.

These methods were proposed to conceal confidential information. In contrast, the WhatsApp application can obstruct the process of law enforcement, as it prevents the revelation of actual information. Anglano et al. investigated disappearing WhatsApp data in digital forensic investigations, aiming to correlate these artifacts with user actions on the device. The study laid a strong foundation for future research, particularly in understanding disappearing messages, after thoroughly examining traditional message artifacts and providing oversight into the WhatsApp structure on Android devices[19].

WhatsApp's disappearing message feature poses a new challenge for digital forensics[28]. This feature is designed to protect user privacy by automatically deleting messages after a specified duration. However, concerns have emerged in Indonesia that this feature could be misused to hide digital evidence that was created and transmitted using WhatsApp[29]. The public is worried that this feature could facilitate infidelity by allowing digital traces to vanish. This feature could also remove digital traces of malware spread through WhatsApp[30], another significant concern for users.

In addition to the disappearing message feature, a similar feature is named "delete for everyone." Both features delete any message on the sender and recipient sides. However, the delete for everyone feature leaves traces, while the disappearing message feature leaves no traces in the chat. This fact emphasizes that screenshots and exports of chat logs are unreliable digital evidence when the disappearing message feature is turned on.

This study uses digital forensics to analyze the artifacts of WhatsApp's disappearing messages based on NIST SP800-101r1 framework. An alternative approach for WhatsApp forensics that does not require rooting while ensuring cost-effectiveness by utilizing the latest open-source tools will be implemented. Furthermore, the forensics methodology will be enhanced by focusing on the latest version of WhatsApp on Android devices.

2. Methodology

2.1 WhatsApp

WhatsApp is an instant messaging application that uses the internet to allow users to communicate with each other. The application operates on a client-server architecture, with the user's device as the client and the WhatsApp server as the server[31]. The server helps facilitate client communication as described in Fig. 1. Messages sent through WhatsApp are temporarily stored on the server until they are received by the recipient or up to 30 days. However, the primary storage for messages is on the user's device.

WhatsApp automatically backs up messages daily and stores them on the client's local device[32]. The backup files are limited to seven with specific name formats. The latest backup file is named "msgstore.db." The previous backups are named "msgstore-yyyy-mm-dd.1.db," indicating their creation time[33]. Figure 2 shows what happens when the backup files are updated. The current "msgstore.db" is renamed to "msgstore-yyyy-mm-dd.1.db" (yellow), the oldest backup is deleted (red) unless its filename has been changed manually (blue), and a new "msgstore.db" is created (green).

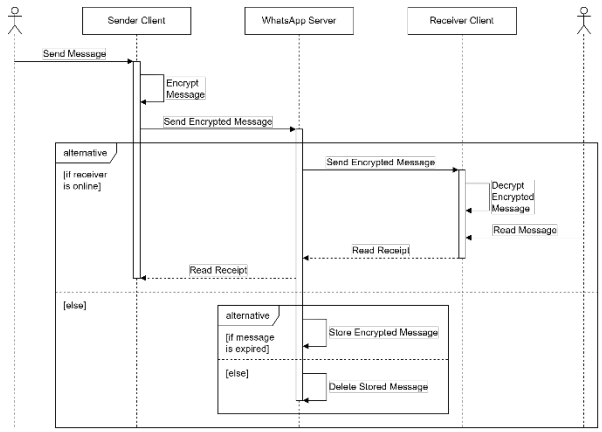

Fig. 1: Message transmission on WhatsApp.

The file extension ".crypt15," shown in Fig. 2, indicates that the backup file is encrypted to ensure data security. Currently, three versions of backup encryption are available: crypt12, crypt14, and crypt15. Although crypt15 is the latest version, it is only implemented when end-to-end backup encryption is enabled.

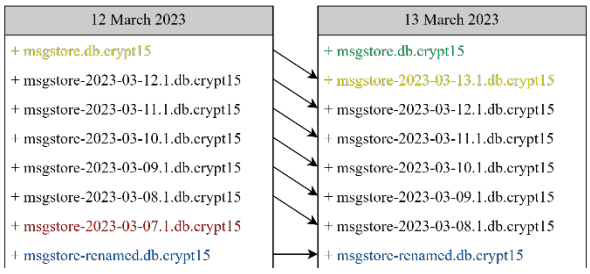

Fig. 2: Local backup on WhatsApp.

2.2 Disappearing Message Feature

Disappearing messages is a WhatsApp feature that allows messages to be stored only for a specified duration, such as 24 hours, 7 days, or 90 days[34]. It is important to note that the disappearing messages functionality will not impact messages exchanged before enabling this feature. WhatsApp has listed the possible effects when this feature is turned on:

1. The message will disappear from the chat if a user does not open WhatsApp in the 24-hour, 7-day, or 90-day period. However, the message preview might remain in notifications until WhatsApp opens.
2. When a user replies to a message, the initial message is quoted. If the initial message is a disappearing message, the quoted text might remain in the chat after the specified duration.
3. If a disappearing message is forwarded to a chat with disappearing messages off, the message will not disappear in the forwarded chat.
4. The disappearing message will be included if a user creates a backup before a message disappears. Backed-up disappearing messages will be deleted when a user restores from a backup.
5. Any media sent in the chat will disappear. However, the phone will save media items if auto-download is turned on.

2.3 Mobile Device Forensics

Mobile device forensics is a branch of digital forensics that focuses on retrieving digital evidence from mobile devices[35]. NIST defines a mobile device as a small, handheld device with a touch-controlled display screen or QWERTY keyboard, enabling communication over a cellular network[36]. NIST SP 800-101r1 provides an in-depth understanding of mobile devices, the technologies involved, and their relationship to forensic steps[37].

The NIST identifies four processes in mobile device forensics, shown in Fig. 3. First, preserving digital evidence is crucial to maintaining its integrity. Second, the acquisition process involves obtaining data through forensic copying of digital evidence. Third, analysis involves examining the data to gather relevant information about the case. Finally, reporting involves presenting the findings and actions taken to ensure the legitimacy of the digital forensic result.

Fig. 3: NIST 800-101r1 Mobile Device Forensic Processes.

As shown in Table 1, two mobile devices are used in our simulation to simulate WhatsApp messages between two users represented by Sherlock and Conan. The devices have different specifications; however, the Android and WhatsApp versions are the same. The devices are pre-configured as below.

1. WhatsApp Messenger is installed from the Google Play Store, and each user creates a WhatsApp account.
2. End-to-end backup encryption on WhatsApp is turned on.
3. Media auto-download on WhatsApp is turned off.
4. Notification history on Android is turned on.

Table 1. Mobile device specifications for simulation.

Specification	Mobile Devices	
	User 1 (Sherlock)	User 2 (Conan)
Models	Vivo V20 SE	Oppo A74
OS	Android 12	
Chipsets	Qualcomm Snapdragon 665	Qualcomm Snapdragon 662
Memory	128 GB, 8 GB RAM	128 GB, 12 GB RAM
Connectivity	Wi-Fi 802.11 a/b/g/n/ac, Bluetooth 5.0, USB Type-C 2.0	
SIM	Dual SIM (Nano-SIM)	
Application	WhatsApp version 2.23.11.77	
WhatsApp Numbers	62851xxxxxx42	62851xxxxxx98

Forensic analysis is conducted in an isolated virtual machine environment using tools shown in Table 2. The environment is pre-configured as below.

1. A pre-built virtual machine image of Kali Linux was installed from the official Kali website.
2. Additional tools not included in Kali Linux were installed from open sources.
3. After tools were installed, network functionality was detached from Kali Linux.
4. A case folder was created as "WA-202306."
5. A CherryTree document was created as "ActivityLogs.ctx."

Table 2. Tools specifications for simulation.

Tools	Version	Purpose of use
Kali Linux	2022.4	Forensic workstation
Sha256sum	9.1	Hashing
Hexdump	2.38.1	Data carving analysis
SQLite DB Browser	3.12.2	Database analysis
CherryTree	0.99.48	Log activities
Android Debug Bridge	1.0.41	Data acquisition
WhatsApp Key/Database Extractor	2022-05-13	Key extraction
WhatsApp Crypt Tools	2023-05-29	Backup file decryption

2.4 Set of Scenarios

Six scenarios are conducted to study how the disappearing message feature affected WhatsApp messages. Each scenario has two conditions: the disappearing message feature is on for 24 hours, and the disappearing message feature is off. Thus, the investigation could be performed by analyzing the differences in WhatsApp messages between the two conditions. Recall that the disappearing message function is time-dependent, so it is essential to have a clearly defined schedule, as shown in Table 3. The purpose of each scenario is described below.

1. Scenario #1: to study how forwarded messages are affected by disappearing message features.
2. Scenario #2: to study how quoted messages are affected by disappearing message features.
3. Scenario #3: to study how media messages are affected by disappearing message features. In this case, the automatically downloaded media is represented by a voice message. In contrast, media that is not automatically downloaded is represented by an image message.
4. Scenario #4: to study how messages are affected by disappearing message features when the recipient is offline. In this case, the recipient will be offline when the message is sent and online after the disappearing message duration has expired.
5. Scenario #5: to study how voice call histories are affected by disappearing message features.
6. Scenario #6: to study how unread messages are affected by disappearing message features.

Table 3. Scenarios schedule in the simulation.

Scenario	Simulation	
	Start Time (UTC+7)	End Time (UTC+7)
#1	2023-06-11 22:05	2023-06-11 22:27
#2	2023-06-12 20:03	2023-06-12 20:04
#3	2023-06-12 20:05	2023-06-12 20:16
#4	2023-06-12 20:24	2023-06-12 20:26
#5	2023-06-13 20:48	2023-06-13 20:51
#6	2023-06-13 20:55	2023-06-12 20:57

2.5 Preservation

Preservation is conducted by following the five actions below.

1. Securing and evaluating the scene: The mobile device and related parts, such as cable chargers, memory cards, and SIM cards found in the scene, are seized and labeled.
2. Documenting the scene: The mobile device conditions, including battery percentage, lock screen, and time, are documented when the device is seized.
3. Isolation: All wireless connections are disabled, and airplane mode is turned on. A wired connection via USB cable Type-C is only used for data acquisition and power charge.
4. Packaging, transporting, and storing evidence: The mobile device is turned on and stored in a zipped pocket attached to a charger.
5. On-site triage: The mobile device is unlocked based on the information given by the owner, the notification log is captured from the settings widget, and USB debugging is enabled under the developer option.

2.6 Acquisition

Data acquisition is conducted by following the six actions below.

1. Establish connection: The mobile device and forensic workstation are connected via USB,

allowing the forensic workstation to control the mobile device via the Android Debug Bridge (ADB).

2. Live acquisition: Notification is dumped using adb and stored as "notification.log." An argument (--noredact) is used to include the notification's text content.
3. Static acquisition: Users can only access WhatsApp data in the "/sdcard/Android/media/com.whatsapp" directory without root privilege. In this case, the adb pull command is used to acquire data from that directory.
4. Key extraction: Encryption keys are extracted using WhatsApp Key/Database Extractor and stored as "sherlock.tar." An argument (--tar-only) is used to include all extractable data in a tar archive.
5. Decryption: WhatsApp Crypt Tool and "find" tools in Kali Linux are used to decrypt backup files. Once decrypted, the files are saved in a "decrypted" folder.
6. File protection: For security purposes, file access is limited by making files read-only and folders write-blocked using the "find" and "chmod" commands. Furthermore, all collected data are hashed using a combination of the "find" and "sha256sum" commands.

2.7 Analysis

The analysis is conducted in the three actions below.

1. Database analysis: SQLite DB Browser is used to study the structure of databases, filtering and querying the data to obtain specific information relevant to the study.
2. File analysis: The format of the files is analyzed, and specific software is utilized to examine their content.
3. Data carving: When analyzing unfamiliar or unsupported files, the "hexdump" command is used to search for patterns within the raw binary data.

2.8 Reporting

Reporting is conducted by documenting the device's condition when it was seized and how the forensic copy was preserved and obtained. The actions taken during the forensics were documented using CherryTree. Furthermore, all results and discussions from the analysis are included to reach a complete conclusion.

3. Results and Discussion

Mobile device forensics is continuously evolving alongside advancement in mobile devices and apps. Numerous studies using various methodologies have been conducted for mobile device forensics. It is important to note that digital forensics is usually conducted on seized evidence. Therefore, it is crucial to consider factors such as method selection, rooting (or not), and choosing between commercial and open-source tools.

As part of this study, the WhatsApp Viewer tool was evaluated to decrypt crypt14 using a known encryption key. However, the tool could not decrypt the message and instead generated an error. Palma et al. developed WhatsApp Crypt Tools to decrypt crypt12, crypt14, and crypt15[41]. These tools have demonstrated their ability to decrypt these databases successfully. Therefore, using current decryption tools in forensic investigations is crucial in accessing previously unreadable message databases.

Based on the acquisition, there are seven folders in com.whatsapp/WhatsApp: "Backups," "Databases," "Media," ".Shared," ".StickersThumbs, " ".Thumbs," and ".trash." However, only the first four folders include files, as shown in Fig. 4. The encrypted files in the "Backups" and "Databases" folders are successfully decrypted using extracted key files: "key" (for crypt12 and crypt14) and "backup_encryption.key" (for crypt15). An image in "Media" is a sent media from Scenario #3, while two images in ".Shared" are pixelated images (allegedly a preview image that Conan sent) and a profile picture. Two audios in "Media" are the sent and received voice messages from Scenario #3. The remaining files are ".nomedia" files (to hide media in the same directory scanned by other applications) or undetermined without additional details.

Figure 4 highlights the diversity of artifacts that can be recovered in WhatsApp forensics, from media files to encrypted databases. Successful extraction of various types of data from multiple directories emphasizes the potential of forensic techniques for recovering seemingly ephemeral or hidden information. This distribution pattern not only underscores the wealth of information potentially hidden in user WhatsApp accounts but also demonstrates the ability of forensics to revive data that users thought was temporary or inaccessible, highlighting the extent to which digital traces are embedded and recoverable.

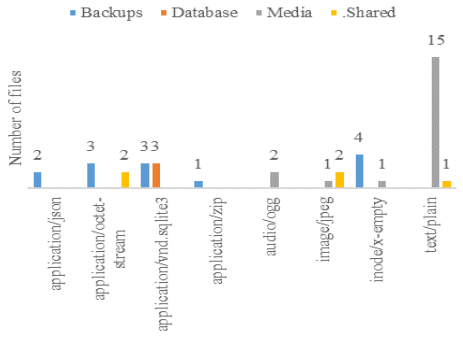

Fig. 4: Distribution of file types recovered from WhatsApp folders.

Regarding the disappearing message feature, related artifacts are backup_settings.json (store auto-download configuration), wa.db (contact database), and message databases. Figure 5 shows three backup versions of the message database; note that the 13 June 2023 backup is missing. On that day, the device was powered off due to the simulation of Scenario #4. As discussed earlier, WhatsApp creates backups at scheduled times. Thus, backup files will not be created when the client device is powered off in the schedule.

Based on database analysis, tables and columns regarding the disappearing message feature are discovered in the message database containing the "disappearing" or "ephemeral" substrings. Table "message_ephemeral" shows all messages affected by the disappearing message feature, including its expired timestamp, while "message_ephemeral_settings" shows the default configuration of the disappearing message feature. In addition, message type 36 in table "message" indicates the configuration change of the disappearing message feature. Six scenarios are reconstructed by running an SQL query that joins two or more tables from the message database, represented by "+" signs, according to Table 4. The message database is reconstructed, and the backup versions were created before the message disappeared.

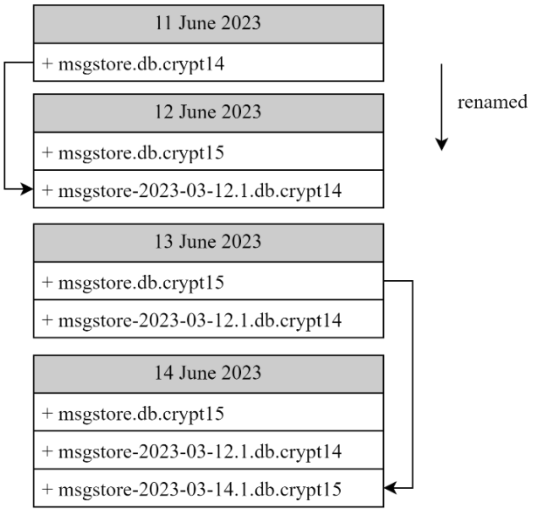

Fig. 5: Backup versions of message database.

Table 4. Joined table for scenario reconstruction.

Table	Scenario					
	#1	#2	#3	#4	#5	#6
jid	+	+	+	+	+	+
chat	+	+	+	+	+	+
message	+	+	+	+	+	+
message_ephemeral	+	+	+	+	+	+
message_forwarded	+	-	-	-	-	-
message_quoted	-	+	-	-	-	-
message_media	-	-	+	-	-	-
call_log	-	-	-	-	+	-

Data carving analysis allowed unread messages to be recovered by analyzing the notification log obtained from the live acquisition. The extras field in the notification object reveals the content of a notification as described in Fig. 6. The disappearing message has been partially revealed from msgstore.db-wal. However, most of the words are cluttered and not in proper sequence, thus requiring further analysis to reconstruct the actual message.

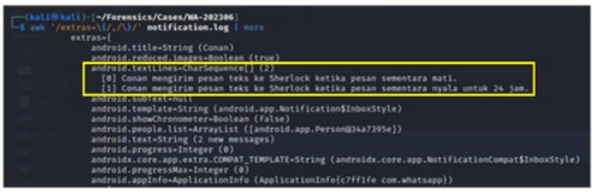

Fig. 6: File analysis of notification.log.

Table 5 summarizes five scenarios (#1, #2, #3, #5, and #6) that were successfully reconstructed from their message history and content because the backup version was discovered before the disappearing message duration expired. Recovered media files are only those files that are sent and received when the temporary message condition is off. Unread messages can be recovered from the notification log even after the duration of the message is temporarily exhausted. On average, the retrieved message is 83.33% of the total data. Heath et al. reviewed the current research into WhatsApp, Snapchat, and Telegram. Among these three applications, WhatsApp holds the largest audience, Telegram is a popular alternative to WhatsApp, and Snapchat was the first to introduce this level of privacy within instant messaging applications. Simulation results on WhatsApp using tools for mobile extractions (XYR and Cellebrite) on iOS and Android devices showed that XRY retrieved 50% of data before disappearing (pre-) and 0% after the disappearing period ended (post-). Cellebrite, on the other hand, retrieves 75% of pre-disappearing and only 42% of data post-disappearing[42]. These results concluded that using unrooted access on Android devices, the current method has better results than the previous study.

Table 5. Summary of findings.

Scenario	Recovered Messages		Artifact(s)
	History	Content	
#1	4/4 (100%)	4/4 (100%)	a. msgstore-2023-06-12.1.db b. msgstore-2023-06-14.1.db c. msgstore.db (backup) d. msgstore.db (extracted)

Scenario	Recovered Messages		Artifact(s)
	History	Content	
#2	2/2 (100%)	2/2 (100%)	a. msgstore-2023-06-14.1.db b. msgstore.db (backup) c. msgstore.db (extracted)
#3	8/8 (100%)	4/8 (50%)	a. msgstore-2023-06-14.1.db b. msgstore.db (backup) c. msgstore.db (extracted) d. audio and image files
#4	1/2 (50%)	1/2 (50%)	a. msgstore.db (backup) b. msgstore.db (extracted)
#5	4/4 (100%)	4/4 (100%)	a. msgstore.db (backup) b. msgstore.db (extracted)
#6	2/2 (100%)	2/2 (100%)	a. msgstore.db (backup) b. msgstore.db (extracted) c. notification logs
Average	**91.67%**	**83.33%**	

4. Conclusions

This research implements an alternative approach for conducting WhatsApp forensics that does not require rooting, which means that the process is not dependent on the brand and model of the device and eliminates the risks associated with rooting. Additionally, the method has been updated to work with the latest app version and utilizes non-commercial tools to reduce costs. Using six scenarios: #1 (forward messages), #2 (quoted messages), #3 (media messages), #4 (offline recipients), #5 (call history), and #6 (unread messages), the simulation obtained artifacts consisting of four message databases, two images, two audios, and one notification log. Based on the analysis, it can be concluded that disappearing messages are stored in the message database on the "message" table with extra columns containing the word "disappearing" or "ephemeral." Results reveal that using unrooted access on Android, 83.33% of disappeared messages could be recovered from backup files and notification logs, while the rest failed due to the missing backup files. The message history found in the message database successfully reconstructs the scenario. However, only part of the message content in Scenario #4 can be recovered by analyzing backup versions of the message database. Despite this, artifacts can still be utilized as digital evidence if the forensic process adheres to NIST or other standards.

For future work, discovering a method to recover disappearing messages is recommended. Further comprehensive studies can be conducted using different approaches and methods to examine the artifacts. Additionally, researching defined protocols and frameworks to analyze and extract data without forensic tools is worth considering.

Acknowledgments

This research is funded by the Directorate of Research Development, Universitas Indonesia, under Hibah PUTI Q2 2023 No. NKB-808/UN2.RST/HKP.05.00/2023.

References

1) W. Huck, "Transforming our world: the 2030 Agenda for Sustainable Development," in: Sustainable Development Goals, 2023. doi:10.5040/9781509934058.0025.
2) R. Imansyah, "Impact of internet penetration for the economic growth of indonesia," *Evergreen*, 5 (*2*) 36–43 (2018). doi:10.5109/1936215.
3) S. Kemp, "Digital 2023: Indonesia," 2023. https://datareportal.com/reports/digital-2023-global-overview-report (accessed May 19, 2023).
4) A. Al-Dhaqm, S.A. Razak, R.A. Ikuesan, V.R. Kebande, and K. Siddique, "A review of mobile forensic investigation process models," *IEEE Access*, 8 (2020). doi:10.1109/ACCESS.2020.3014615.
5) H. Uddin, and M.K. Barai, "Will digital revolution be disruptive for the inclusive finance in bangladesh? the case of the microfinance industry," *EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy*, 09(4) 909–923 (2022). doi.org/10.5109/6622878
6) M. Kar, and N. Bothra, "Pandemic and indian education: evolving perspectives from higher education," *Evergreen*, 10(1) 18–28 (2023). doi.org/10.5109/6781030
7) R. Mustajab, "WhatsApp masih menjadi media sosial terfavorit di indonesia," *Dataindonesia.Id*, (2023).
8) V.M. Rumata, and A.S. Sastrosubroto, "The Indonesian Law Enforcement Challenges over Encrypted Global Social Networking Platforms," in: 2018 International Conference on Computer, Control, Informatics and Its Applications: Recent Challenges in Machine Learning for Computing Applications, IC3INA 2018 - Proceeding, 2018. doi:10.1109/IC3INA.2018.8629528.
9) Z. Prihatini, and A.N.K. Monavita, "Ahli forensik digital beberkan riwayat komunikasi teddy minahasa dan anak buahnya," *Kompas.Com*, 1–2 (2023). https://megapolitan.kompas.com/read/2023/03/02/12085781/ahli-forensik-digital-beberkan-riwayat-komunikasi-teddy-minahasa-dan-anak (accessed May 19, 2023).
10) Muhammad Zakaria Pasaribu, Yusni Khairul Amri, and Dian Marisha Putri, "Pragmatic presupposition of netizen comments on instagram related to teddy

minahasa case," *LingLit Journal Scientific Journal for Linguistics and Literature*, 3 (*4*) (2023). doi:10.33258/linglit.v3i4.824.
11) E.S. Hasibuan, and A. Syauket, "Efforts to eradicate narcotics in the national police: a case study of teddy minahasa," *International Journal of Social Service and Research*, 3 (*4*) (2023). doi:10.46799/ijssr.v3i4.346.
12) R. Zaikin, and O. Vanunu, "Reverse Engineering WhatsApp Encryption for Chat Manipulation and More," Islander EI, 2019. https://www.blackhat.com/us-19/briefings/schedule/#reverse-engineering-whatsapp-encryption-for-chat-manipulation-and-more-15540 (accessed June 9, 2023).
13) Republik Indonesia, "Undang-undang nomor 11 tahun 2008," (*11*) (2008).
14) M.S. Sumathi, J. Shruthi, V. Jain, G.K. Kumar, and Z.Z. Khan, "Using artificial intelligence (ai) and internet of things (iot) for improving network security by hybrid cryptography approach," *Evergreen*, 10 (*2*) 1133–1139 (2023). doi:10.5109/6793674.
15) A. Gera, and V. Vyas, "Message security enhanced by bit cycling encryption and bi-lsb technique," *Evergreen*, 9 (*3*) 845–852 (2022). doi:10.5109/4843115.
16) A.S.M. Shaiden, S. Islam, and K. Subramaniam, "Android based digital steganography application using lsb and psnr algorithm in mobile environment," *Evergreen*, 8 (*2*) 421–427 (2021). doi:10.5109/4480724.
17) D. Wijnberg, and N.A. Le-Khac, "Identifying interception possibilities for whatsapp communication," *Forensic Science International: Digital Investigation*, 38 (2021). doi:10.1016/j.fsidi.2021.301132.
18) A.S.M. Shaiden, S. Islam, and K. Subramaniam, "Android based digital steganography application using lsb and psnr algorithm in mobile environment," *Evergreen*, 8 (*2*) 421–427 (2021). doi:10.5109/4480724.
19) C. Anglano, "Forensic analysis of whats app messenger on android smartphones," *Digit Investig*, 11 (*3*) 201–213 (2014). doi:10.1016/j.diin.2014.04.003.
20) Y. Salem, M. Owda, and A.Y. Owda, "An experimental approach for locating whatsapp digital forensics artefacts on windows 10 and the cloud," *International Journal of Electronic Security and Digital Forensics*, 15 (*3*) (2023). doi:10.1504/IJESDF.2023.130662.
21) F. Alief, Y. Suryanto, L. Rosselina, and T. Hermawan, "Analysis of autopsy mobile forensic tools against unsent messages on whatsapp messaging application," *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2020-October 26–30 (2020). doi:10.23919/EECSI50503.2020.9251876.
22) A. Sengupta, A. Singh, and B.M. Vinjit, "A platform independent and forensically sound method to extract whatsapp data from mobile phones," *International Journal of Electronic Security and Digital Forensics*, 15 (*3*) 259–280 (2023). doi:10.1504/IJESDF.2023.130657.
23) T. Hermawan, Y. Suryanto, F. Alief, and L. Roselina, "Android forensic tools analysis for unsend chat on social media," *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2020*, 233–238 (2020). doi:10.1109/ISRITI51436.2020.9315364.
24) D.S.I. Utomo, Y. Prayudi, and E. Ramadhani, "Forensic web analysis on the latest version of whatsapp browser," *Journal of Computer Networks, Architecture and High Performance Computing*, 5 (*1*) (2023). doi:10.47709/cnahpc.v5i1.2286.
25) F.E. Salamh, U. Karabiyik, and M.K. Rogers, "Asynchronous forensic investigative approach to recover deleted data from instant messaging applications," in: 2020 International Symposium on Networks, Computers and Communications, ISNCC 2020, Institute of Electrical and Electronics Engineers Inc., 2020. doi:10.1109/ISNCC49221.2020.9297227.
26) H. Fayyad-Kazan, S. Kassem-Moussa, H.J. Hejase, and A.J. Hejase, "Forensic analysis of whatsapp sqlite databases on the unrooted android phones," *HighTech and Innovation Journal*, 3 (*2*) 175–195 (2022). doi:10.28991/HIJ-2022-03-02-06.
27) M. Shadeed, L.A. Arram, and M. Owda, "Forensic analysis of 'whatsapp' artifacts in android without root," *Advances in Science, Technology and Engineering Systems Journal*, 7 (*2*) 127–132 (2022). doi:10.25046/aj070212.
28) H. Heath, Á. MacDermott, and A. Akinbi, "Forensic analysis of ephemeral messaging applications: disappearing messages or evidential data?," *Forensic Science International: Digital Investigation*, 46 (2023). doi:10.1016/j.fsidi.2023.301585.
29) E. Yanwardhana, "Waduh! fitur whatsapp ini disebut bikin selingkuh lebih aman," (2022). https://www.cnbcindonesia.com/tech/20220625173835-37-350330/waduh-fitur-whatsapp-ini-disebut-bikin-selingkuh-lebih-aman.
30) R.N. Chaterine, and D. Prabowo, "Bareskrim tangkap 13 tersangka kasus penipuan apk andorid, kerugian capai rp 12 miliar," *Kompas.Com*, 1–1 (2023). https://nasional.kompas.com/read/2023/01/19/18211941/bareskrim-tangkap-13-tersangka-kasus-penipuan-apk-andorid-kerugian-capai-rp (accessed May 19, 2023).
31) C. Cressler, "Understanding whatsapp's architecture & system design," (2021). https://www.cometchat.com/blog/whatsapps-architecture-and-system-design (accessed June 20,

2023).
32) WhatsApp, "About whatsapp," *About WhatsApp*, (n.d.). https://www.whatsapp.com/about (accessed November 30, 2022).
33) kipjr, "[Q&A] whatsapp structure and information," 1–1 (2014). https://forum.xda-developers.com/t/q-a-whatsapp-structure-and-information.2984056/ (accessed June 20, 2023).
34) WhatsApp Blog, "Introducing disappearing messages on whatsapp," *WhatsApp Blog*, 1–1 (2020). https://blog.whatsapp.com/introducing-disappearing-messages-on-whatsapp (accessed November 30, 2022).
35) P. Reedy, "Mobile Device Forensics," in: Encyclopedia of Forensic Sciences: Volume 1-4, Third Edition, 2022. doi:10.1016/B978-0-12-823677-2.00240-3.
36) R. Ayers, S. Brothers, and W. Jansen, "Guidelines on Mobile Device Forensics," Gaithersburg, MD, 2014. doi:10.6028/NIST.SP.800-101r1.
37) A. Ajijola, P. Zavarsky, and R. Ruhl, "A Review and Comparative Evaluation of Forensics," 2014.
38) F. Alief, Y. Suryanto, L. Rosselina, and T. Hermawan, "Analysis of Autopsy Mobile Forensic Tools Against Unsent Messages on WhatsApp Messaging Application," in: International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Institute of Advanced Engineering and Science, 2020: pp. 26–30. doi:10.23919/EECSI50503.2020.9251876.
39) A. Sengupta, A. Singh, and B.M. Vinjit, "A platform independent and forensically sound method to extract whatsapp data from mobile phones," *International Journal of Electronic Security and Digital Forensics*, 15 (*3*) (2023). doi:10.1504/IJESDF.2023.130657.
40) T. Hermawan, Y. Suryanto, F. Alief, and L. Roselina, "Android Forensic Tools Analysis for Unsend Chat on Social Media," in: 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2020, Institute of Electrical and Electronics Engineers Inc., 2020: pp. 233–238. doi:10.1109/ISRITI51436.2020.9315364.
41) D. Palma, "WhatsApp crypt tools," (2023). https://github.com/ElDavoo/wa-crypt-tools (accessed May 19, 2023).
42) H. Heath, Á. MacDermott, and A. Akinbi, "Forensic analysis of ephemeral messaging applications: disappearing messages or evidential data?," *Forensic Science International: Digital Investigation*, 46 (2023). doi:10.1016/j.fsidi.2023.301585.