WhatsApp Mobile Applications in the Lens of Digital Forensics: Deciphering the Msgstore.db.crypt14 File

Wahyu Adi Prabowo[1,*], Fadi Mohsen[2]
and Siti Rahayu Selamat[3]

[1]*Department of Informatics, Telkom University, D.I Panjaitan No. 128, Banyumas, 53147, Indonesia*
[2]*Information Systems Group, Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence, University of Groningen, 9712 CP Groningen, The Netherlands*
[3]*Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia*
E-mail: wahyup@telkomuniversity.ac.id; f.f.m.mohsen@rug.nl; sitirahayu@utem.edu.my
[*]*Corresponding Author*

Received 17 December 2024; Accepted 10 August 2025

Abstract

This study investigates the forensic analysis of WhatsApp's Msgstore.db.crypt14 file, focusing on rooted and non-rooted devices, which pose unique challenges in data extraction and decryption. This research leverages forensic tools such as WhatsApp-Key-Database Extractor, Binwalk, and Mobile Edit to demonstrate a systematic approach for retrieving and analyzing encrypted data, uncovering hidden content, and extracting valuable metadata. The findings highlight the consistency of WhatsApp's encryption mechanisms across rooted and non-rooted devices, emphasizing the

Journal of Cyber Security and Mobility, Vol. 14_4, 823–848.
doi: 10.13052/jcsm2245-1439.1443

importance of using multiple forensic tools for comprehensive analysis. Key contributions include insights into WhatsApp's metadata, encryption keys, and the implications of phone number or device changes on data security. This study advances the field of digital forensics by offering practical methodologies for analyzing encrypted mobile messaging data, providing a foundation for future research into improving forensic tools and addressing privacy and ethical considerations.

Keywords: Msgstore.db.crypt14, WhatsApp's, digital forensics, data extraction, data storage.

1 Introduction

Mobile messaging applications such as WhatsApp, WeChat, and Telegram have revolutionized digital communication by enabling rapid engagement [1], promoting collaboration [2], and facilitating the exchange of varied content [3]. Among these platforms, WhatsApp stands out as one of the most widely used messaging applications globally, with studies indicating it has over two billion active users as of 2024 [3]. This widespread adoption has made WhatsApp an essential tool in both personal and professional communication environments [4]. WhatsApp provides a widely accessible platform free of charge [5], facilitating group chats and supporting several media formats, including images, videos, and voice communications [6]. The extensive use has transformed communication patterns, surpassing geographical limitations [7] and promoting real-time connections, community development [8], and collaboration [9].

In digital forensic investigations, WhatsApp databases like the Msgstore.db.crypt14 file are essential components [10, 11]. This encrypted database contains essential information, encompassing text messages, multimedia files, phone records, and metadata from user activities. The encrypted format of Msgstore.db.crypt14 presents considerable obstacles for forensic investigators in data extraction and analysis. Unlocking critical evidence in cases of cyberbullying, fraud, and terrorism [12] requires specialized tools and techniques, emphasizing the importance of thoroughly understanding data structure, storage mechanisms, and analysis methods [13–15].

Although extensive investigations have examined WhatsApp's Msgstore.db.crypt data files [2, 7, 11, 12], a significant gap remains in understanding the successful extraction and analysis of Msgstore.db.crypt14 files from non-rooted cellphones. Current methodologies primarily concentrate

on rooted devices, undermining the integrity of forensic data and frequently resulting in data loss [19, 20]. Furthermore, the majority of studies concentrate on earlier iterations of WhatsApp databases, specifically Msgstore.db.crypt12, whereas the more intricate Msgstore.db.crypt14 files remain insufficiently examined [21–23]. Addressing these gaps is crucial for improving forensic investigations and ensuring the secure retrieval of encrypted WhatsApp data without compromising the device's security settings.

This study aims to implement alternative techniques for extracting and analyzing encrypted WhatsApp data from non-rooted devices. A notation system is introduced to define key terms, forensic tools, and data structures used, ensuring clarity and consistency. This system is essential for representing the encrypted file, encryption and decryption processes, and tools used to examine the Msgstore.db.crypt14 file. Detailed explanations of the notations are provided to support a thorough understanding of the forensic process and study findings.

This study's findings have significant implications for digital forensics. The techniques developed for non-rooted devices provide practical, accessible methods for retrieving WhatsApp data, enabling forensic investigators to conduct more precise and effective investigations. These methods reduce data loss and support law enforcement and forensic examiners in identifying and preserving essential digital evidence. Additionally, this study establishes a foundation for future improvements in WhatsApp data analysis, offering insights that could refine forensic tools, advance encryption and data storage approaches, and enhance analysis across other messaging platforms.

To provide a structured understanding of this study, the paper is organized as follows: Section 1 introduces the significance of mobile messaging applications like WhatsApp in digital forensics, emphasizing the challenges posed by the encrypted Msgstore.db.crypt14 file and defining the research gap. Section 2 details the materials and methods, describing the forensic tools and systematic processes used to collect, examine, and analyze data from both rooted and non-rooted devices. Section 3 presents the results and discussion, focusing on three experimental scenarios: (1) comparing data extraction from rooted versus non-rooted devices, (2) exploring the impact of encryption key management during device or SIM card changes, and (3) analyzing the effectiveness of various forensic tools in examining the file's structure, metadata, and hidden content. Section 4 concludes the paper by summarizing the key findings, discussing limitations, and suggesting directions for future research. This structure provides a comprehensive examination of the forensic analysis of encrypted WhatsApp data.

1.1 Related Work

Significant progress has been made in WhatsApp forensics, with numerous studies exploring techniques for extracting and analyzing WhatsApp data. Early research, such as studies by [12, 24], primarily focused on rooted devices and used tools like Autopsy, WhatsApp Viewer, and Hex Editor for data extraction. These investigations demonstrated how forensic investigators could retrieve critical information from older WhatsApp databases, specifically `Msgstore.db.crypt12` files, though this often required rooted access, which risks altering or destroying crucial data.

Forensic tools like Belkasoft Evidence, Oxygen Forensic, and Elcomsoft WhatsApp Explorer have been assessed for their capability to analyze WhatsApp datasets. Specifically, studies conducted by [18, 19] evaluated the efficacy of these tools in decrypting and studying previous iterations of `Msgstore.db.crypt` files. However, these tools were not optimized for processing the newer `Msgstore.db.crypt14` format, which uses advanced encryption techniques. Additionally, while effective on rooted devices, their functionality is limited on non-rooted smartphones, leaving a gap in the analysis of encrypted data on devices with factory security settings intact.

Issues with non-rooted devices remain a notable research gap. Previous studies, such as those by [17, 23], proposed automated extraction techniques for earlier database versions but did not offer comprehensive methods for analyzing `Msgstore.db.crypt14` files without rooting the device. These constraints highlight the necessity for alternate approaches that maintain data integrity while allowing investigators to access encrypted WhatsApp information. Furthermore, studies like those by [21, 22] have highlighted the risks associated with rooted devices, such as data corruption and compromised forensic evidence, emphasizing the need for methods focused on analyzing non-rooted devices.

This research presents methodologies for analyzing `Msgstore.db.crypt14` files specifically on non-rooted smartphones, while also considering rooted devices where applicable. By leveraging open-source forensic tools such as WhatsApp-Key-Database Extractor, Binwalk, and Mobile Edit, this study addresses a critical gap in mobile forensics by providing methods that minimize data loss and preserve forensic integrity without requiring device modification. These techniques not only improve accessibility for WhatsApp data extraction but also establish a foundation for future advancements in analyzing encrypted messaging applications.

2 Material and Method

In this research, a systematic forensic process was implemented, consisting of four primary stages: collection, examination, analysis, and reporting, as shown in Figure 1. The notations used to represent key data structures and forensic tools throughout this section are introduced to ensure clarity and consistency.

The notations in Table 1 represent key concepts and tools used throughout this forensic analysis:

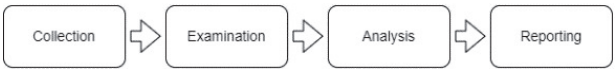

Figure 1 Research method.

Table 1 Notation table for WhatsApp file analysis

Notation	Description
F	Represents the WhatsApp `Msgstore.db.crypt14` file, an encrypted database file.
K	Denotes the encryption key used to encrypt and decrypt the file.
E(F, K)	Refers to the encryption of file F using the encryption key K.
D(E(F, K), K)	Represents the decryption process where the encrypted file E(F, K) is decrypted using the key K.
M	Messages within the WhatsApp file.
C	Contacts stored in the database.
T	Timestamps associated with messages or activities.
MD	Metadata information such as backup dates or encryption versions.
T1	`WhatsApp-Key-Database-Extractor`, used to extract encryption keys and databases from WhatsApp on Android devices for forensic investigations and data analysis.
T2	`Hex Editor`, software tool for viewing and editing binary files in hexadecimal format, enabling byte-level data modification.
T3	`Binwalk`, firmware analysis tool that extracts embedded file systems and identifies file types within firmware images.
T4	`Mobile Edit`, software tool for mobile forensics, facilitating data extraction from mobile devices such as text messages and call logs.
T5	`WhatsApp Viewer`, tool to view and analyze contents of WhatsApp backup files, including chat messages, media, and contact information.
T6	`DB Browser for SQLite (DB4S)`, visual tool for managing and manipulating SQLite databases, allowing easy creation, modification, and querying of databases.

Throughout the forensic process, these notations are referenced to clarify each stage: collection, examination, analysis, and reporting. Consistently using these notations keeps the discussion organized and precise, allowing for a clearer understanding of each methodological step.

2.1 Forensic Process Stages

2.1.1 Collection stage

The collection stage focused on identifying and acquiring potential evidence sources relevant to WhatsApp forensic analysis. The hardware materials used are listed in Table 2, and the software materials used for data extraction are described in Table 3.

The primary target for this stage was the `Msgstore.db.crypt14` file (F) and its associated encryption key (K) retrieved from two Android devices: a non-rooted Samsung Galaxy A5 running Android 8.0 and a rooted Xiaomi 9T running Android 12. The devices were connected to the computer via USB. Specialized forensic tools such as *WhatsApp-Key-Database Extractor* and *Mobile Edit* were employed to facilitate the extraction process. The *WhatsApp-Key-Database Extractor* was specifically used to retrieve the `Msgstore.db.crypt14` file and its encryption key (K) from the devices.

The output of this stage was a fully extracted `Msgstore.db.crypt14` file and its corresponding encryption key, which were backed up securely using third-party software to ensure the integrity and reliability of the collected data. This step completed the acquisition process, preparing the extracted data for further examination and analysis.

In the final step of this stage, the collected `Msgstore.db.crypt14` file (F) and its encryption key (K) were prepared for decryption. These files were securely transferred to forensic analysis tools to enable subsequent stages of investigation, ensuring that the data remained intact and ready for detailed analysis.

The primary target was the `Msgstore.db.crypt14` file (F) and its associated encryption key (K), retrieved from two Android devices: a non-rooted

Table 2 Hardware material

Hardware	Description	Version
Samsung Galaxy A5 with simcard	Unrooted device	Android Version 8
Xiaomi 9t with simcard	Rooted device	Android Version 12
USB Connection	Connecting device	-
Laptop, AMD Ryzen 16GB RAM	Analysis devices	-

Table 3 Forensic analysis tools

Software	Description	Version	Functionality	Purpose
`Whatsapp Key Database Extractor`	Extracts encryption keys and databases from WhatsApp on Android devices for forensic investigations and data analysis.	2020	Extracts passwords and encryption keys from WhatsApp	Necessary for opening files and accessing the information stored in the `Msgstore.db.crypt14` file
`Hex Editor`	Software tool for viewing and editing binary files in hexadecimal format, enabling byte-level data modification.	2.5.0.0	Views and edits files in hexadecimal format	Helps analyze the structure and content of the `Msgstore.db.crypt14` file in more detail
`Binwalk`	Firmware analysis tool that extracts embedded file systems and identifies file types within firmware images.	2.3.4	Analyzes binary files	Helps uncover important components in files like `Msgstore.db.crypt1` and understand the structure and metadata contained within
`Mobile Edit`	Software tool for mobile forensics, facilitating data extraction from mobile devices such as text messages and call logs.	8	Extracts various types of data from Android devices	Helps uncover WhatsApp message files, including `Msgstore.db.crypt1`, as well as related files such as images, videos, and audio files
`Whatsapp Viewer`	Tool to view and analyze contents of WhatsApp backup files, including chat messages, media, and contact information.	1.9	Reads and views encrypted WhatsApp message files	Allows for the viewing of conversations, attachments, and contact information
`DB Browser for SQLite (DB4S)`	Visual tool for managing and manipulating SQLite databases, allowing easy creation, modification, and querying of databases.	3.12.2	Manages and analyzes SQLite databases	Useful for uncovering tables within the file and viewing data such as messages, contacts, and other stored information

Samsung Galaxy A5 running Android 8.0 and a rooted Xiaomi 9T running Android 12. The devices were connected to the computer via USB.

For this stage, the forensic tools *WhatsApp-Key-Database Extractor* and *Mobile Edit* were used to extract the `Msgstore.db.crypt14` file (F) and its associated encryption key (K). Retrieving the encryption key was not a straightforward process, as it depended on the compatibility of the tool with the device and the Android version. *WhatsApp-Key-Database Extractor* facilitated this step by accessing specific files stored in the device's internal memory, such as key files associated with WhatsApp backups. The process required a full backup of the device's data, which was then analyzed to locate and extract the encryption key.

Once the `Msgstore.db.crypt14` file and its encryption key were acquired, the decryption process was initiated. This process was represented mathematically as:

$$D(E(F, K), K) = \{M, C, T, MD\}$$

The decryption process utilized tools such as *DB Browser for SQLite (DB4S)* and *Hex Editor* to decode the encrypted contents of the file. The encryption key (K) was applied using the same internal mechanisms that WhatsApp employs to manage encrypted backups. The process involved matching the extracted key with the encrypted data and validating the decryption output through iterative testing, ensuring the extracted data aligned with the expected format.

During decryption, challenges such as key mismatch or data corruption were encountered. To address these issues, forensic examiners cross-verified the extracted key against the device's metadata and ensured that the backup file matched the correct encryption key. After the decryption process was completed, the file's contents—including messages (M), contacts (C), timestamps (T), and metadata (MD)—were made accessible for further analysis using tools such as *WhatsApp Viewer* and *DB Browser for SQLite*.

2.1.2 Examination Stage

The Examination Stage begins with the decrypted `Msgstore.db.crypt14` file and associated data, which were obtained during the Collection Stage. The focus of this stage is to inspect the contents of the decrypted file and prepare it for detailed forensic analysis.

During the Examination Stage, the extracted content is validated and organized into a format suitable for further forensic interpretation. If inconsistencies or gaps in the data are identified, additional verification may involve

reconnecting the devices to the forensic workstation. For instance, supplementary checks on file integrity or device-specific settings may be performed. However, no further modifications or extractions beyond verification were conducted in this stage.

The goal of this stage is to ensure that the decrypted data is accurate, well-structured, and ready for use in subsequent analysis and reporting stages. By focusing on the extracted content, the Examination Stage serves as a bridge between the initial data collection and the deeper forensic analysis that follows. This ensures that the data is not only well-organized but also primed for further correlation with investigative leads in the next stage.

2.1.3 Analysis Stage

In the analysis stage, a comprehensive examination of the extracted data was conducted, including keyword searches and data interpretation. The forensic tools were used to interpret and correlate the evidence, uncover patterns, and establish relationships. In order to explore data extraction methods, three experimental scenarios focusing on the `Msgstore.db.crypt14` file were conducted.

Scenario 1 – Comparison of Data Extraction Results: The first scenario involved a comparison of data extraction results obtained from rooted and non-rooted smartphones. The objective of this scenario was to identify variations in the extracted data and understand the potential impact of device rooting on the quality and quantity of recovered data.

Scenario 2 – Management of Cipher Keys in WhatsApp: This scenario focused on understanding the management of cipher keys in WhatsApp and their dependence on SIM cards. It involved transferring the `Msgstore.db.crypt14` file to USB storage and directly extracting the same file on the smartphone. The results from both methods were compared to identify potential variations in the extracted data.

Scenario 3 – Analysis with Binwalk, Mobile Edit, and WhatsApp Viewer: This scenario evaluated the reliability and accuracy of various forensic tools, including Binwalk, Mobile Edit, and WhatsApp Viewer, in retrieving data from Android smartphones. The objective was to identify the most effective tools for data extraction and analysis.

2.1.4 Reporting stage

In the reporting stage, a detailed forensic report was compiled, providing a comprehensive summary of the investigation. The report presented the

analysis results, key conclusions, and an in-depth discussion of the research process. Through this rigorous forensic methodology, the findings were validated for accuracy and reliability. This ensured the research met the requirements of its intended audience, including digital forensic investigators, law enforcement agencies, and academic researchers.

3 Results and Discussion

This section presents the results and analysis derived from the experiments outlined earlier in Section 2. The findings are structured around three scenarios, each focusing on data extraction outcomes, encryption mechanisms, and the effectiveness of forensic tools.

Two Android smartphones were used in the experiments: a non-rooted Samsung Galaxy A5 (Android 8.0) and a rooted Xiaomi 9T (Android 12). Both devices were connected to a forensic workstation via USB to retrieve the `Msgstore.db.crypt14` file and its associated encryption key (*K*) using the *WhatsApp-Key-Database Extractor*. The file was then analyzed using forensic tools tailored to the specific objectives of each scenario. Although the same devices were used across all scenarios, the experimental setups, tools, and processes were adjusted to address the distinct goals of each scenario.

3.1 Scenario 1: Comparison of Data Extraction Results

After extracting the Msgstore.db.crypt14 file (F) and its associated encryption key (K) during the experimentation setup, Scenario 1 focused on comparing the encrypted files retrieved from rooted ((R(F)) and non-rooted (NR(F)) devices. The analysis evaluated three primary aspects: (1) file structure, including timestamps messages (M), contacts (C), timestamps (T), and metadata (MD).

The files were analyzed in their encrypted state using the Hex Editor (T2) to examine raw data attributes. Figures 5 and 6 illustrate the similarities in structure and metadata between the rooted and non-rooted files, demonstrating consistent encryption mechanisms and data organization.

The results revealed no significant differences between the files extracted from rooted and non-rooted devices. The metadata attributes were identical, and showed no variation. This finding confirms that the rooting status of a device does not affect the integrity or completeness of encrypted forensic data.

Figure 2 Hexadecimal representation of the Msgstore.db.crypt14 file (rooted device).

Figure 3 Hexadecimal representation of the Msgstore.db.crypt14 file (non-rooted device).

The `Msgstore.db.crypt14` file extracted from a non-rooted device (Xiaomi 9T) was analyzed using a *Hex Editor*, providing a raw hexadecimal and ASCII view. Similar to the file extracted from a rooted device, the non-rooted file exhibits an identical structure, consistent encryption metadata, and a uniform organization of encrypted message content. This observation confirms that rooting a device does not affect the integrity or storage mechanism of WhatsApp's encrypted backup files.

The analysis of the provided images highlights that `Msgstore.db.crypt14` files from both rooted and non-rooted devices share similar structural attributes, with no discernible differences. These files are presented in hexadecimal format alongside their ASCII interpretations, revealing raw binary data that potentially represents encrypted information or a serialized database. The presence of readable strings and structured patterns within the files indicates embedded metadata or message-related content, such as timestamps, unique identifiers, or other information used by WhatsApp.

This consistency in data patterns across rooted and non-rooted devices demonstrates the uniformity of WhatsApp's encryption and storage mechanisms. Such findings are critical for forensic validation, as they ensure that data integrity and structure are preserved regardless of the device's rooting status.

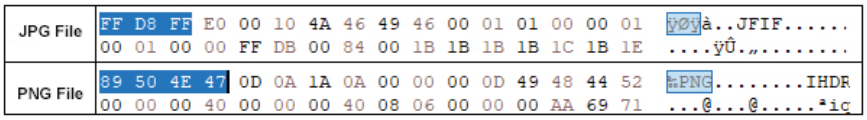

Figure 4 File extension JPG and PNG.

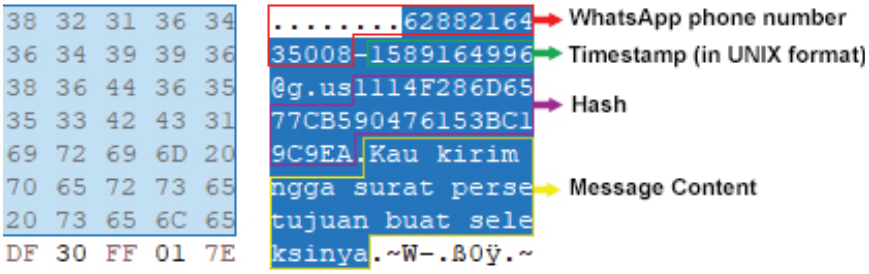

Figure 5 Hexadecimal representation of metadata and message content.

In analyzing the metadata of files such as JPG and PNG (Figure 4) within the extracted Msgstore.db.crypt14 file, both rooted and non-rooted devices revealed embedded information associated with chat messages and sender details.

The analysis found no significant differences between files extracted from rooted and non-rooted phones. For example, the Msgstore.db.crypt14 file's metadata often includes rich contextual information, as demonstrated in Figure 5. This metadata reveals that chat messages are embedded within media files, such as JPG and PNG, which are exchanged during WhatsApp conversations. The extracted data contains a phone number (6288216435008), a timestamp in UNIX format (1589164996, corresponding to Monday, May 11, 2020, 2:43:16 AM), a unique session hash (1114F286D6577CB590476153BC19), and the actual message content ('Kau kirim ngga surat persetujuan buat seleksinya'). This consistent pattern across rooted and non-rooted devices highlights the uniformity in WhatsApp's encryption and storage mechanisms, providing critical insights for reconstructing conversations, identifying associated media files, and verifying sender details.

Results obtained from Scenario 1 support these research findings, showing that there are no significant differences between the `Msgstore.db.crypt14` files extracted from rooted (*R(F)*) and non-rooted (*NR(F)*) smartphones:

$$S1 : R(F) \approx NR(F)$$

This indicates that the encryption $E(F, K)$ and storage mechanisms employed by WhatsApp are consistent across device configurations. This key observation offers insights into the strength of WhatsApp's data protection measures, regardless of the device's rooting status.

Moreover, the research revealed that the `Msgstore.db.crypt14` file stores not only WhatsApp messages (*M*) but also valuable metadata (*MD*) such as backup dates and the encryption version used by WhatsApp. This metadata is crucial for digital forensic investigations as it provides additional contextual information about the data, aiding in understanding the timeline and integrity of the backups. Using *Hex Editor* (*T2*), the raw binary data of the `Msgstore.db.crypt14` file was thoroughly examined and analyzed.

Although the initial appearance of encrypted data $E(F, K)$ in a hex editor may seem indecipherable, this data can be transformed into a comprehensible format through the process of decryption $D(E(F, K), K)$. This complex process uncovers hidden information within the encrypted data, allowing researchers to extract valuable insights. The decryption of the encrypted file allowed for the interpretation of both the messages (*M*) and the accompanying metadata (*MD*), offering valuable data for forensic analysis and research.

3.2 Scenario 2: Management of Cipher Keys in WhatsApp

This research scenario focused on the effects of data migrations and phone number alterations on file encryption, specifically targeting the `Msgstore.db.crypt14` file (*F*). The *WhatsApp-Key-Database Extractor* was used to retrieve the encryption key (*K*) and databases from the two Android devices used in this study: a non-rooted Samsung Galaxy A5 and a rooted Xiaomi 9T. Notably, this extraction process does not require rooting the Android device, making it an effective solution for users wishing to recover their WhatsApp data without modifying the device's system. However, the success of this tool can depend on both the device and the software versions in use, as updates to WhatsApp or security protocols may impact the extraction. The encryption key (*K*) retrieved from the unrooted Samsung Galaxy A5 is shown in Figure 6.

The extraction of the key, represented as an encrypted string (*K*), is a pivotal step in the research. This key is crucial for the decryption of the

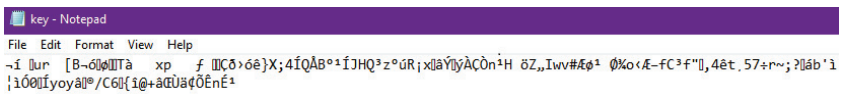

Figure 6 The encryption key retrieved from the unrooted Samsung Galaxy A5.

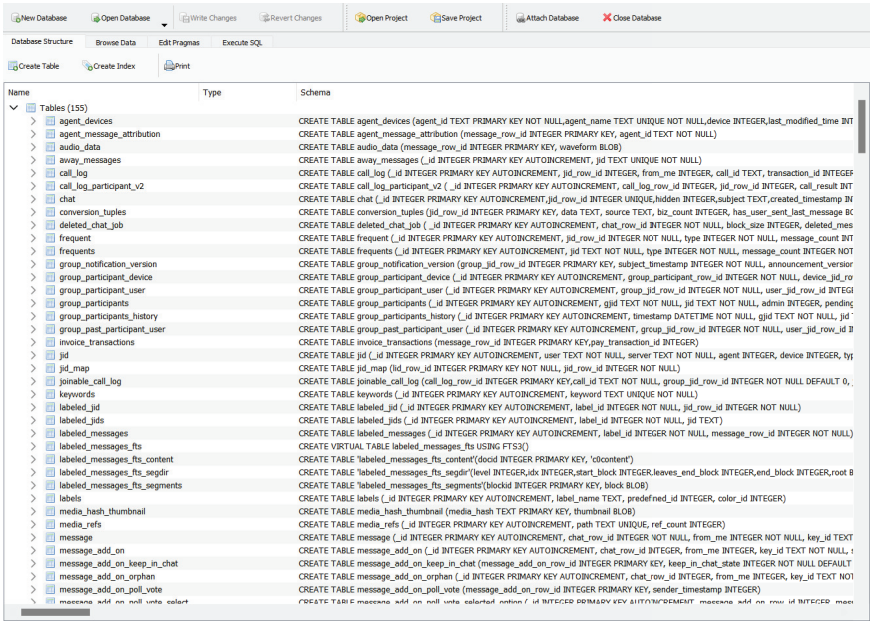

Figure 7 Database of Msgstore.db.crypt14.

`Msgstore.db.crypt14` backup files $E(F, K)$. With the encryption key at hand, decryption of the backup files becomes possible using appropriate decryption tools. This process allows access to the contents of the backup files, enabling further analysis. The decryption process is represented as:

$$D(E(F, K), K)$$

This decryption unlocks the contents of the `Msgstore.db.crypt14` file, allowing it to be viewed in *DB Browser for SQLite (DB4S)*, as illustrated in Figure 7.

Each time a user alters their phone number or migrates to a new device, a new encryption key (*K_new*) is generated to secure their files. This key is essential for preserving the confidentiality and integrity of the encrypted data. However, it is important to note that the encryption key cannot be transferred between different phone numbers or devices. As shown in Figure 5, if the user attempts to decrypt the files using the previous encryption key (*K1*) after switching back to the original number or device, the decryption will fail, as:

$$E(F, K1) \neq D(E(F, K1), K\_new)$$

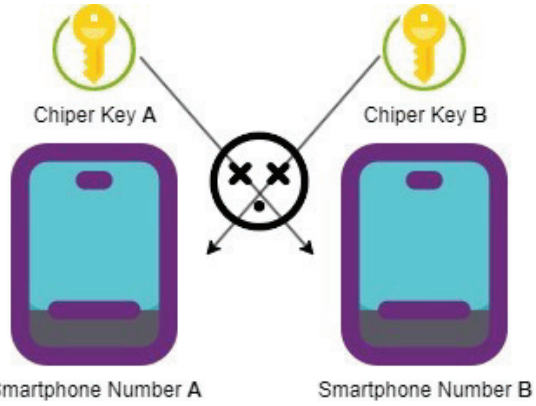

Figure 8 Unsuccessful attempt at changing phone number to another smartphone.

This indicates that the old encryption key is incompatible with the new encryption key generated after a phone number change.

As in the case of mobile phone, a variety of phone models or operating systems may employ distinct encryption algorithms or security protocols, thereby necessitating diverse methods or procedures for the acquisition of the encryption key. Consequently, as depicted in Figure 6, contemplating and adapting to the specific prerequisites of each phone or device is imperative for users when handling the encryption key, as this will facilitate seamless and secure file encryption and decryption.

In the scenario of altering phone numbers or devices, this process requires a thorough understanding of the encryption system and careful handling of the encryption key. Users must grasp that the encryption key is essential to safeguarding their personal data. By understanding that the encryption key is non-transferable between different phone numbers or devices, users can undertake necessary measures to ensure that their encrypted data remains secure and impervious to unauthorized access. In this context, it's essential for users to follow the procedures specified by their phone model or operating system when changing phone numbers or devicess. This approach ensures the accuracy of the generated encryption key and the correct encryption of files following changes to phone numbers or devices. By adjusting for the specific requirements of each phone or device, users can ensure that the file encryption and decryption processes are fully functioning and secure in diverse environments. Several findings emerged during the extraction process. A key discovery was the message database (M), which allowed us to access users' conversation history, including text messages, images, videos,

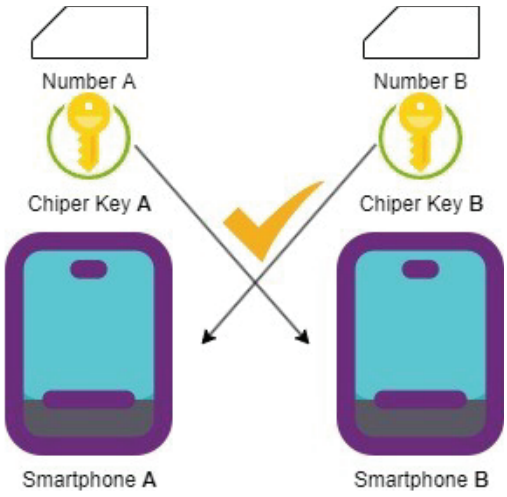

Figure 9 Successful attempt at changing phone number to another smartphone.

and other files, as shown in Figure 7. Analysis of this database provided information on discussion topics.

In this experiment, two devices were used: a non-rooted Samsung Galaxy A5 and a rooted Xiaomi 9T, each equipped with unique SIM cards and WhatsApp installations. The initial step involved extracting the encryption keys (K) and encrypted `Msgstore.db.crypt14` files (F) from both devices using the *WhatsApp-Key-Database Extractor*. Both files were successfully decrypted, enabling access to user messages (M) and metadata (MD). The SIM cards on both devices were then replaced with new ones, and the extraction process was repeated. The new encryption keys (K_{new}) were successfully retrieved, but attempts to decrypt the previously extracted files (F) using the new keys (K_{new}) were unsuccessful. This confirms that the encryption keys are uniquely linked to the SIM card in use during file generation. The analysis demonstrated that while the decryption process with the original keys (K) was successful, the altered configuration of the SIM card rendered the old keys incompatible. This underscores the strength of WhatsApp's encryption mechanism, which prevents unauthorized decryption when key or device configurations are changed.

Furthermore, as depicted in Figure 8, the msgstore.db file, which resulted from the extraction process in scenario 1, contains user contact details, including names, phone numbers, and other related information. This file can be accessed using the DB Browser for SQLite (DB4S) software. Such

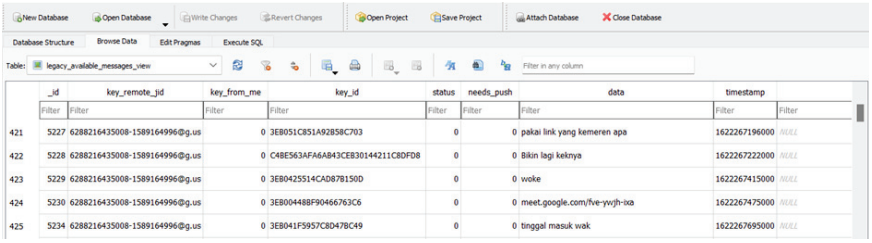

Figure 10 Messaging information from Msgstore.db file.

contact data prove instrumental in identifying linkages between users and charting existing communication networks. In addition, image files and other media transmitted or received via WhatsApp were delved into. Through the analysis of this media content, categories of data disseminated, emerging visual patterns, and topics frequently discussed within the conversations were discerned.

The findings shed light on the technical complexities of file encryption during data transfers. Factors such as the Android device and the presence of encryption keys influenced the encryption status of the Msgstore.db.crypt14 file. The WhatsApp-Key-Database Extractor proved highly effective in extracting the necessary encryption key (K) to decrypt the file and access its contents for further analysis.

3.3 Scenario 3: Analysis with Binwalk, Mobile Edit, and WhatsApp Viewer

This section presents a comparison of various forensic tools used for analyzing the `Msgstore.db.crypt14` file (F), focusing on key aspects such as its structure, metadata (*MD*), concealed content, and data extraction capabilities. The evaluation was guided by a set of defined criteria: File Structure Analysis, Metadata Extraction, Hidden Data Detection, Message Analysis, Ease of Use, Key Use Case, and Recovery of Deleted Messages.

Binwalk (T_1) became an essential tool in the analysis, demonstrating strengths in File Structure Analysis, Metadata Extraction, and Hidden Data Detection. Using *Binwalk* (Figure 9), the hierarchical structure of the `Msgstore.db.crypt14` file (F) was identified, providing a clear understanding of its organization. Relevant metadata (MD), including creation dates and file size, was successfully extracted, offering a comprehensive overview of the file's contextual properties. Additionally, the advanced analysis techniques implemented in *Binwalk* (T_1) enabled the detection of

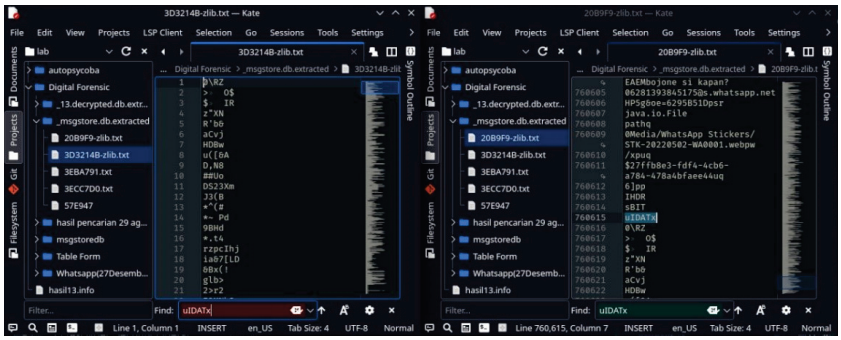

Figure 11 Analysis using Binwalk tools.

hidden data and the recognition of file types utilized within the WhatsApp database.

Furthermore, *Binwalk* (T_1) facilitated Data Extraction and Presentation by enabling the retrieval of the file's contents, granting access to deeper levels of data for detailed analysis. However, it is important to note that the results may vary depending on the specific characteristics and structure of the file. Despite this, *Binwalk*'s ability to meet multiple comparison criteria makes it a valuable tool for forensic investigations involving encrypted databases like `Msgstore.db.crypt14`.

Mobile Edit (*T2*) emerged as another essential tool in this research, specifically for the analysis of the `Msgstore.db.crypt14` file (*F*). The mobile editing capabilities were augmented by extracting key metadata (*MD*) such as creation time, file size, conversation content (*M*), and other relevant details from smartphones, as shown in Figure 10. This offered valuable insights into the file's characteristics and enabled a more detailed forensic analysis. Furthermore, *Mobile Edit* (*T2*) helped reveal hidden content within the file, making it an essential tool for uncovering concealed information.

Through the integration of Binwalk (T1) and Mobile Edit (T2), a comprehensive understanding of the file's structure and composition was achieved, addressing the File Structure Analysis criterion. While Binwalk laid the foundation by identifying the file's structure and metadata, Mobile Edit complemented this by extracting deeper, more specific information. This synergy highlights the tools' ability to collectively fulfill the Comprehensive Tool Comparison criterion, demonstrating their value in conducting a meticulous forensic analysis of the Msgstore.db.crypt14 file (F).

Furthermore, *WhatsApp Viewer* (*T3*) (Figure 11) emerged as an invaluable tool in the research, particularly for analyzing the extracted data from the

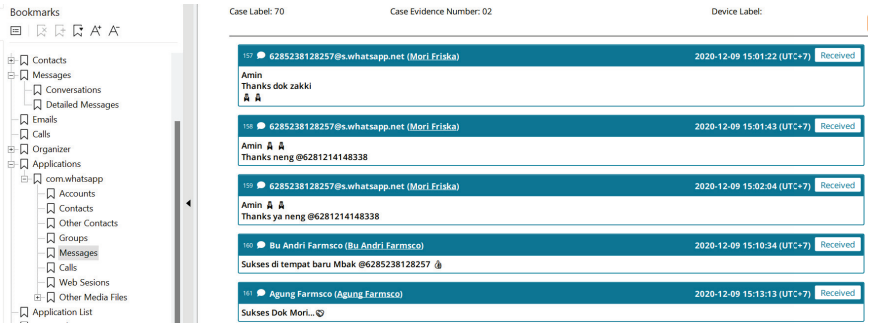

Figure 12 Analysis using mobile edit tools.

Figure 13 Analysis using WhatsApp viewer tools.

`Msgstore.db.crypt14` file (*F*). This tool, specifically designed for accessing and analyzing WhatsApp message content (*M*), proved to be highly effective. *WhatsApp Viewer* (*T3*) enabled easy viewing of conversations, attachments, and contact information associated with each message, providing insights into WhatsApp communication patterns. The tool's search function allowed for the pinpointing of specific keywords or phrases within the messages, facilitating a more targeted approach to data analysis. A noteworthy finding from the investigation was *WhatsApp Viewer's* (*T3*) ability to recover deleted messages from the database, providing access to content that may have been removed from the WhatsApp application. This ability underscores the efficacy of *WhatsApp Viewer* (*T3*) in revealing concealed or deleted information, highlighting its utility in forensic analysis.

Table 4 Performance evaluation of forensic Tools

Evaluation Criteria	Binwalk (T1)	Mobile Edit (T2)	WhatsApp Viewer (T3)
File Structure Analysis	Identifies file structure and metadata	Extracts key metadata and details	Limited to WhatsApp database, focuses on message structure
Metadata Extraction	Provides general file metadata (creation date, size)	Extracts detailed metadata (creation time, size, and conversation content)	Metadata tied to messages and attachments
Hidden Data Detection	Detects hidden data and identifies embedded files	Helps uncover hidden content within files	Recovers deleted messages from the database
Message Analysis	Not applicable	Provides conversation details via metadata	Direct access to and analysis of WhatsApp messages
Ease of Use	Command-line interface, advanced technical skills required	Graphical interface, moderately user-friendly	Graphical interface, highly user-friendly
Key Use Case	Analyzing file structures, identifying hidden files	Detailed examination of metadata and hidden content	Recovering deleted messages, analyzing message content
Recovery of Deleted Messages	Not applicable	Not applicable	Yes, recovers deleted messages effectively

Through the integration of WhatsApp Viewer (T3) with complementary forensic tools such as Binwalk (T1) and Mobile Edit (T2), a holistic analysis of the extracted data from the Msgstore.db.crypt14 file (F) was achieved. Each tool contributed uniquely to the evaluation criteria, addressing aspects such as File Structure Analysis, Metadata Extraction, Hidden Data Detection, Message Analysis, and Recovery of Deleted Messages (refer to Table 4). Binwalk (T1) excelled in identifying file structures and detecting hidden data, while Mobile Edit (T2) offered detailed metadata extraction and conversation context. WhatsApp Viewer (T3) stood out in message analysis and the recovery of deleted messages, providing direct insights into WhatsApp communication patterns. Collectively, these tools facilitated the discovery of critical forensic data, supporting the broader objectives of this research.

3.4 Discussion

In the first scenario, the process of extracting data from the `Msgstore.db.crypt14` file (*F*) on smartphones was undertaken. The findings revealed no significant disparities in the file's content between rooted (*R(F)*) and non-rooted (*NR(F)*) smartphones, indicating uniformity in device usage. This comparative analysis, facilitated by *Hex Editor* (*T2*), further supported this observation, showing a consistent data pattern across both devices. The `Msgstore.db.crypt14` file functions as an encrypted backup of WhatsApp data, encapsulating text dialogues (*M*) from the mobile device. The encryption of this file is designed to safeguard WhatsApp dialogues from unauthorized access, ensuring the privacy and security of the stored data. Furthermore, the file contains metadata (*MD*) about each backup, including the backup date and encryption version used, providing additional forensic insights. This information is essential for comprehending WhatsApp's data storage systems and aids in forensic investigation.

In the second scenario, focused on the management of cipher keys in WhatsApp, the impact of data transfers and phone number changes on file encryption was investigated, specifically for the `Msgstore.db.crypt14` file ($E(F, K)$). The *WhatsApp-Key-Database Extractor* was used to retrieve encryption keys (K) and databases from both rooted and unrooted Android devices. This tool proved capable of extracting keys from non-rooted devices, offering an effective solution for recovering WhatsApp data without requiring device modification. However, its effectiveness may vary depending on the device model and software version in use.

When users change their phone number or upgrade to a new device, a new encryption key (K_{new}) is generated, rendering previous keys (K_1) invalid for decrypting new data. As illustrated in Figure 5, attempts to revert to an old phone number demonstrate the non-transferability of encryption keys. This highlights the need for careful encryption key management to ensure data security. Users should adhere to the procedures specified by their phone model or operating system when changing phone numbers or devices, as this ensures the accurate generation of encryption keys and the correct encryption of files.

Furthermore, the process of altering phone numbers or devices underscores the importance of understanding encryption systems. Different phone models or operating systems may employ varied encryption algorithms or security protocols, requiring specific methods to retrieve or manage encryption keys. This emphasizes the need for users to adopt device-specific

approaches to maintain the integrity and security of their encrypted data.

In the third scenario, Analyzing Outcomes Using Various Forensic Tools, several forensic tools were compared to analyze the `Msgstore.db.crypt14` file (*F*) in order to gain insights into its structure, metadata (*MD*), hidden content, and data extraction capabilities. *Binwalk* (*T1*) played a pivotal role in identifying the file's structure, extracting key metadata, and recognizing the file types used in the WhatsApp database. This tool was essential for detecting hidden data within the file. *Mobile Edit* (*T2*) was essential for extracting and analyzing data from cellphones, including metadata (*MD*) such as file creation timestamps, file size, and conversation specifics (*M*). Additionally, *WhatsApp Viewer* (*T3*) streamlined the process of accessing WhatsApp message content, simplifying the viewing of conversations, attachments, and contact information. This tool enabled a detailed analysis of WhatsApp communications, including the recovery of deleted messages, which contributed further to the forensic investigation.

4 Conclusion

This study analyzed the `Msgstore.db.crypt14` file using forensic tools, demonstrating the effectiveness of a multi-tool approach in digital forensic investigations. Tools such as *Binwalk*, *Hex Editor*, *WhatsApp Viewer*, and *Mobile Edit* provided valuable insights into encrypted data, metadata, and hidden content, emphasizing the critical role of combining diverse tools in forensic analysis.

The primary contribution of this research is showcasing the systematic application of these tools to retrieve messages, multimedia, and metadata, while highlighting the significance of WhatsApp's encryption mechanisms. These findings enhance the ability to reconstruct communication and recover digital evidence from encrypted messaging apps.

However, this study has limitations, including tool effectiveness varying with device or software versions and a focus on a specific WhatsApp database version. Future research should explore multiple database versions, address legal and ethical considerations, and validate findings through real-world forensic applications. The advancement of forensic tools and methodologies will improve the reliability of data extraction and analysis while addressing privacy and legal challenges.

By integrating diverse forensic tools, this research contributes to the advancement of digital forensic techniques, providing a foundation for more

comprehensive investigations into mobile messaging applications. Ongoing innovation in this field will support law enforcement and strengthen forensic capabilities.

References

[1] J. M. Katy Jordan, *RAPID EVIDENCE REVIEW: Messaging apps, SMS & social media*. GlobalEdTechHub, 2020.

[2] C. M. Tang and A. Bradshaw, "Instant messaging or face-to-face? How choice of communication medium affects team collaboration environments," *E-Learning and Digital Media*, vol. 17, no. 2, 2020. doi:10.1177/2042753019899724.

[3] Statista, "Most popular global mobile messenger apps as of April 2024, based on number of monthly active users," *Statista*, 2024. Available at: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/. Accessed: November 9, 2024.

[4] C. L. Wang, "New frontiers and future directions in interactive marketing: Inaugural Editorial," *Journal of Research in Interactive Marketing*, vol. 15, no. 1, 2021. doi:10.1108/JRIM-03-2021-270.

[5] A. Seufert, F. Poignée, T. Hoßfeld, and M. Seufert, "Pandemic in the digital age: analyzing WhatsApp communication behavior before, during, and after the COVID-19 lockdown," *Humanities and Social Sciences Communications*, vol. 9, no. 1, 2022. doi:10.1057/s41599-022-01161-0.

[6] B. Suárez-Lantarón, Y. Deocano-Ruíz, N. García-Perales, and I. S. Castillo-Reche, "The Educational Use of WhatsApp," *Sustainability*, 2022. doi:10.3390/su141710510.

[7] B. Hagedoorn, E. Costa, and M. Esteve-del-Valle, "Photographs, Visual Memes, and Viral Videos: Visual Phatic News Sharing on WhatsApp during the COVID-19 Pandemic in Spain, Italy, and The Netherlands," *Digital Journalism*, 2023. doi:10.1080/21670811.2023.2250395.

[8] H. Verma, J. Mlynář, C. Pellaton, M. Theler, A. Widmer, and F. Evéquoz, "WhatsApp in Politics?!: Collaborative Tools Shifting Boundaries," in *Lecture Notes in Computer Science*, 2021. doi:10.1007/978-3-030-85623-6_37.

[9] I. Mashiah, "The relationship between public-relations and journalists in WhatsApp technology," *Public Relations Review*, vol. 47, no. 5, 2021. doi:10.1016/j.pubrev.2021.102117.

[10] I. F. Rahmadi, "WhatsApp group for teaching and learning in Indonesian higher education what's up?," *International Journal of Interactive Mobile Technologies*, vol. 14, no. 13, 2020. doi:10.3991/ijim.v14i13.14121.

[11] D. Sudiana, C. H. Nuruddin, M. Rizkinia, and D. Husna, "Forensic Analysis of WhatsApp Disappearing Message on Unrooted Android Using Mobile Device Forensics Methodology NIST SP 800-101r1," *Evergreen*, vol. 11, no. 1, pp. 516–524, 2024. doi:10.5109/7172316.

[12] F. Yudha, A. Luthfi, and Y. Prayudi, "A proposed model for investigating on web WhatsApp application," *Advanced Science Letters*, vol. 23, no. 5, 2017. doi:10.1166/asl.2017.8308.

[13] 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.

[14] F. Yudha, E. Ramadhani, D. Sudyana, and W. N. Hamzah, "A custom recovery approach for physical forensic imaging of android device," in *AIP Conference Proceedings*, 2023. doi:10.1063/5.0114894.

[15] R. Umar, I. Riadi, and G. Maulana, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 12, 2017. doi:10.14569/ijacsa.2017.081210.

[16] C. Morris, R. E. Scott, and M. Mars, "WhatsApp in clinical practice—The challenges of record keeping and storage. A scoping review," *International Journal of Environmental Research and Public Health*, 2021. doi:10.3390/ijerph182413426.

[17] R. Cents and N. A. Le-Khac, "Towards a new approach to identify WhatsApp messages," in *Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2020)*, 2020. doi:10.1109/TrustCom50675.2020.00259.

[18] M. Iqbal and I. Riadi, "Forensic WhatsApp based Android using National Institute of Standard Technology (NIST) Method," *International Journal of Computer Applications*, vol. 177, no. 8, 2019. doi:10.5120/ijca2019919443.

[19] T. Almehmadi and O. Batarfi, "Impact of android phone rooting on user data integrity in mobile forensics," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 12, 2018. doi:10.14569/IJACSA.2018.091279.

[20] M. Hassan and L. Pantaleon, "An investigation into the impact of rooting android device on user data integrity," in *Proceedings of the 2017 7th International Conference on Emerging Security Technologies (EST 2017)*, 2017. doi:10.1109/EST.2017.8090395.

[21] M. Moreb, "Mobile Forensic Investigation for WhatsApp," in *Practical Forensic Analysis of Artifacts on iOS and Android Devices*, 2022. doi:10.1007/978-1-4842-8026-3_9.

[22] R. Khweiled, M. Jazzar, A. Eleyan, and T. Bejaoui, "Using SQLite Structure Analysis To Retrieve Unsent Messages On WhatsApp Messaging Application," in *2022 International Conference on Smart Applications, Communications and Networking (SmartNets 2022)*, 2022. doi:10.1109/SmartNets55823.2022.9993988.

[23] M. Mirza, F. E. Salamh, and U. Karabiyik, "An Android Case Study on Technical Anti-Forensic Challenges of WhatsApp Application," in *8th International Symposium on Digital Forensics and Security (ISDFS 2020)*, 2020. doi:10.1109/ISDFS49300.2020.9116192.

[24] K. Alissa et al., "A comparative study of WhatsApp forensics tools," *SN Applied Sciences*, vol. 1, no. 11, 2019. doi:10.1007/s42452-019-1312-8.

Biographies

Wahyu Adi Prabowo holds a Bachelor's degree in Informatics Engineering from the Islamic University of Indonesia, a Master's degree in Business Administration from Universitas Gadjah Mada, and a Master's degree in Informatics Engineering from the Islamic University of Indonesia. Since August 2024, he has been pursuing his Ph.D. at National Yang Ming Chiao Tung University, Taiwan. His research interests focus on cybersecurity and digital forensics. He is currently serving as an Assistant Professor at Telkom University, Indonesia.

Fadi Mohsen obtained his BSc in Computer Information Systems from the University of Jordan, Jordan. In 2008, he was awarded a Fulbright Scholarship, which enabled him to pursue an MSc in Computer Science at the University of Colorado at Colorado Springs, USA. He completed his Ph.D. in Computing and Informatics in 2016 at the University of North Carolina at Charlotte, USA. He is currently an Assistant Professor at the University of Groningen, the Netherlands. His research focuses on usable security, mobile and web security, moving target defense, and security analytics.

Siti Rahayu Selamat is currently an Associate Professor at the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia. She holds a Ph.D. in Computer Science with a specialization in Digital Forensics. Her research interests include network forensics, cyber terrorism, cyber violent extremism, intrusion detection, and penetration testing. She is an active member of the INSFORNET research group, with a focus on malware analysis, criminal behavior profiling, and cyber violent extremism.