Journal of Integrated and Advanced Engineering (JIAE)
Vol. 3, No. 1, March 2023: 7-22
http://asasijournal.id/index.php/jiae
http://doi.org/10.51662/jiae.v3i1.70

Identification of WhatsApp Digital Evidence on Android Smartphones using The Android Backup Application Package Kit (APK) Downgrade Method

Sulisdyantoro Deny*, Marza Ihsan Marzuki
Department of Electrical Engineering, Faculty of Engineering, Universitas Mercu Buana, Indonesia

Abstract
The use of WhatsApp for actions that lead to unlawful acts is a serious matter that needs to be proven in court. Android and the WhatsApp messaging application continue to update their features and security to provide maximum service and protection to its users, such as the WhatsApp database encryption using crypt14. With crypt14 encryption on the WhatsApp database, investigations of WhatsApp digital evidence against Electronic Evidence (BBE) require an acquisition and extraction method to identify artefacts relevant to digital evidence needs. The National Institute Standard Technology (NIST) reference methodology, from the collection, examination, and analysis to reporting stages, has become a widely used framework for digital forensics against BBE. The Android Backup Application Package Kit (APK) Downgrade method can decrypt the WhatsApp database crypt14 to become a solution that can be used in the framework of mobile forensics to answer the needs of investigations into certain criminal cases, including data that users have deleted. With the Cellebrite tools, the Android Backup Application Package Kit (APK) Downgrade method can identify approximately 651% more artefacts than the Android Backup and logical acquisition methods using the FinalData and MobilEdit tools.

Keywords:
Android;
APK downgrade;
Cellebrite;
Smartphone;
WhatsApp;

Article History:
Received: July 27, 2022
Revised: February 23, 2023
Accepted: February 28, 2023
Published: March 25, 2023

Corresponding Author:
Sulisdyantoro Deny
Department of Electrical Engineering, Faculty of Engineering, Universitas Mercu Buana, Indonesia
Email:
deny.sulisdyantoro@gmail.com

INTRODUCTION

Currently, the role of the internet is increasingly important in the global world's social, economic and political life. Indonesia also experienced this increase. The survey results of the Indonesian Internet Service Providers Association (APJII) 2019-2020 Q2 [1], the penetration of the number of internet users in Indonesia is 196.71 out of a total population of 266.91 million Indonesians or around 73.7%. And in the survey, in 2019, smartphone devices dominated internet use, with a percentage of 95.4%. Instant Messenger is an application often used to communicate, replacing the role of Short Message Services (SMS) [2]. WhatsApp is one of the most popular instant messenger applications and can be used on mobile devices and computers [3]. The number of smartphone users is increasing, especially on the Android platform [4].

WhatsApp has many features, such as telephone, group chat, video calling, file sending, and voice messaging [5]. WhatsApp places the messaging app far ahead of all other messaging apps like Facebook Messenger, WeChat, Viber, Apple Business Chat, or Telegram regarding user count. WhatsApp has many features, such as telephone, group chat, messaging, video calling, file sending, and voice messaging. WhatsApp has become a reference in digital forensics in Indonesia [6]. Figure 1 shows that WhatsApp is in the top three as a widely used platform.

Android smartphone forensics has evolved, offering significant opportunities and exciting challenges. Some of these crimes include using the sophistication of the Android smartphone to commit crimes such as fraud, gambling, pornography, corruption, drug networks, to murder cases. In several recent crime cases, such as in the trial of Nainggolan's investigation [7] and in a follow-up hearing on the false news of Sarumpaet, [8], using WhatsApp conversations as evidence in court. This shows that from a forensic investigation perspective, the WhatsApp application can store evidence data that can be used in court as evidence. Therefore, using the Forensic approach, it is very important to have a methodology and framework to parse WhatsApp application data on both active and deleted Android devices. This study will describe the mechanism for opening database files and backup files from the WhatsApp application on an Android smartphone. This research is expected to contribute to a framework that can be applied to perform smartphone forensics by finding and analyzing artefacts in the WhatsApp application on Android smartphones using the Android Backup APK Downgrade acquisition method. With the forensic approach used, it is not only possible to restore existing conversations and data but also data and conversations that have been deleted.

MATERIAL AND METHODS

Related Work

Several previous studies to identify WhatsApp digital evidence have been carried out previously on Android-based smartphones. Zhang [9] explained that there is no encrypted database on a rooted phone while the database is encrypted on a non-rooted phone. Rahadhian [10] using the Integrated Digital Forensic Investigation Framework (IDFIF) version 2 (two) and Oxygen Forensic Suite, MobilEdit Express, and Andriller tools, can identify WhatsApp Desktop content that contains cybercrime. Unlike the case with Umar [3] comparing the Belkasoft Evidence tools, WhatsApp Key DB/Extractor uses the NIST framework to make acquisitions with physical and logical methods. As a result, Belkasoft Evidence has the highest index number, and WhatsApp Key/DB Extractor is superior in terms of cost. At the same time, Oxygen Forensic is superior in obtaining WhatsApp artefacts through logical and physical acquisitions.

Yuliani [11], using Oxygen forensics, and Andriller obtained evidence of smartphone artefacts such as chat sessions, avatars, and contacts in the WhatsApp application.

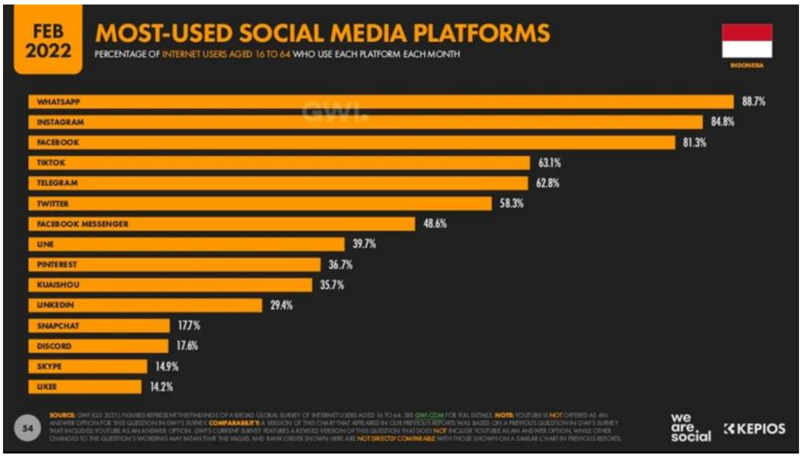


Figure 1. WhatsApp User Statistics

Then, Widiandana [12] acquired with Oxygen Forensic, analyzing the acquisition results using Text Mining, Cosine Similarity and NIST framework methods. It was found that there are similarities between words in digital evidence and words that are negative will help identify cyber bullying actions.

Several studies using the FTK Imager tool by Marfianto [13] have obtained artefacts in the form of WhatsApp text message chat conversation sessions and can also get other media files encrypted by crypt12. Riadi [14], with the live forensic method on WhatsApp desktop, obtained digital evidence in the form of texts of WhatsApp conversations that occurred between the suspect and the victim, which can be used as digital evidence related to the online shop fraud case that occurred. Then Kumang [15] by using ProDiscover Basic Tools, AccessData FTK Imager, WhatsApp Viewer, and DB Browser for SQLite and WhatsApp encryption on crypt8, getting evidence artefacts in the form of chat sessions, avatars, contact numbers on the WhatsApp application, voice notes, profile photo, the identity of the owner of the WhatsApp account and also can get other media files and most importantly encrypted backup database files. Meanwhile, Saputra [16], with FTK Imager and live forensic methods, used the extracted data from the acquisition, explored the characteristics of WhatsApp Messenger users according to the chat content and labelled using the crowdsourcing method. Finally, Wirara [17] used XRY and Encase Mobile Forensic to obtain WhatsApp digital evidence even though the device was not rooted/jailbroken first.

Anggraini [18] uses recovery tools Dr Fone for Android to recover deleted WhatsApp messenger data, but the media URL cannot be opened because it is encrypted by WhatsApp, while WhatsApp messenger database analysis uses DB Browser for SQLite. On the other hand, a study by Akbar [19] explained that it could generate the required data, such as log timestamps, photos sent, call logs, and messages sent and received. Tools used Using Internet Protocol with Wireshark and Live Memory. In contrast to Mirza [20] who proposed the possibility of anti-forensic techniques for the WhatsApp application through two hypothetical case scenarios, namely by disabling the delete feature for everyone when the sender is blocked from the contact list and conducting an application demo that can recover deleted messages even after the status is blocked.

Meanwhile, for research using Cellebrite UFED tools, Hussein [21] conducted experiments on Android smartphones with internal storage, no-rooting and Cellebrite UFED tools. This study explains how to extract the Crypt key from the WhatsApp application to decrypt the database and extract artefacts on the android system without rooting the device. With these conditions and the development of WhatsApp application updates to improve services, features and security, it is inversely proportional to mobile forensics tools which have limitations with the large variety of Android phones with the development of each of the modifications of the Android version according to the characteristics of each brand, So in this study, it is proposed to use the Android APK downgrade backup method by extracting WhatsApp application data using Android backup (android backup) which contains the Android file system. In the acquisition process, the version of the WhatsApp application used (*.apk file) is temporarily downgraded to the previous version so that data can be extracted. Then the version used will be restored at the end of the extraction process. Thus, using the Android APK Downgrade backup method through the extraction process of the database encrypted by WhatsApp can be made possible to run after the WhatsApp version is downgraded. The acquisition results will be analyzed using the Cellebrite Physical Analyzer tool.

Material

The specifications of the software used for digital evidence analysis, in this case, are as follows: Android Smartphone Samsung Galaxy Note 9 (OS. Android 10), Data cable, Windows 10 and platforms for acquisition and analysis, Cellebrite UFED version 7.50.0.137 for acquisition, Cellebrite Physical Analyzer version 7.52.0.36 for analysis, and WhatsApp application version 2.22.3.75. Table 1 lists the devices used.

Methods

The National Institute of Standards and Technology (NIST) is a non-regulatory body of the Technology Administration section of the United States Department of Commerce, which issues the publication of NIST SP 800-86, which divides the process of digital forensics into four stages. The four stages are as follows [27, 28, 29, 30]:

Figure 2 shows the stages of the digital forensic process, starting from collection, examination, analysis and reporting. The collection is the first stage in the digital forensics process to identify potential data sources before acquiring the data. At this stage, physical and digital evidence will be safeguarded, and its integrity will be ensured at every stage of the investigation process by following established guidelines and procedures. Identification by preserving BBE is the most important procedure in digital forensic investigations [9]. Forensic investigators must document every event and activity without or with little change to the evidence in digital forensic rules. Every change must be well documented so that the validity and integrity of the evidence are maintained and can be accounted for in court. The examination is the stage of obtaining evidence in accordance with standard procedures, which is preceded by examining the data, which includes the assessment and extracting of information from previously collected data by using a combination of automatic and manual methods to assess and extract interesting data while maintaining data integrity. The analysis is the process of analyzing data that can identify people, places, items, and related events so that conclusions can be drawn by interpreting the digital evidence that has been identified. Unreadable digital evidence is secured or used directly for presentation in court. Therefore, forensic investigators need to use forensic tools to analyze the collected data [9]. This stage aims to obtain useful information to answer the questions that are the driving force in conducting the collection and examination, namely by analyzing the data obtained in the previous stage to identify the source of the crime and motive using justifiable methods/techniques. Legally, supported by adequate/qualified evidence, it can be accepted and ultimately prove the person responsible for the crime and/or deny the alleged crime.

Table 1. Simulation device

NO	Simulation device	Description
1.	Samsung Galaxy Note 9 SM-N960F	Android 10
2.	*WhatsApp*	Instant messaging application version 2.22.3.75
3.	Workstation	Microsoft Windows 10 Pro 64 Bit, Intel i9-7900X, 64 GB RAM
4.	USB Cable	connect a smartphone to a workstation with a USB type C cable

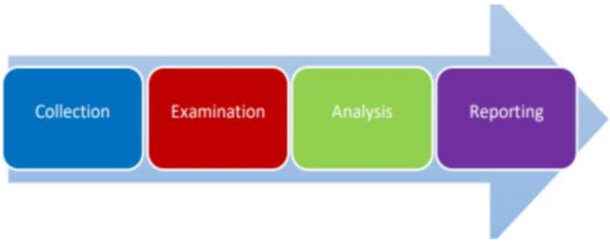


Figure 2. Number and Figure Caption

Finally, Reporting is preparing and presenting the information from the analysis phase. This final phase reports the results of the analysis, describes the actions used, explains how tools and procedures were selected, determines what other actions need to be taken (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improves existing security controls), and provides recommendations for improvement of policies, guidelines, procedures, tools, and other aspects of the forensic process [27, 28, 29, 30].

RESULTS AND DISCUSSION

This research was conducted using an Android smartphone installed with the WhatsApp messaging application version 2.22.3.75. In the scenario that investigators find evidence of a Samsung Galaxy Note 9 smartphone with an unrooted version of Android 10 used in this research.

Simulation

This research simulation was carried out at the Indonesian Attorney's Digital Forensic Laboratory. In the simulation, it takes an Android smartphone device, Samsung Galaxy Note 9, installed the WhatsApp messaging application version 2.22.3.75 then, devices communicate and send chats, pictures and video calls. The next stage is to carry out the acquisition and extraction of the two smartphone devices using a PC or laptop with Windows OS. After imaging, the analysis process is carried out, and then a report is made on the evidence.

Stages of collection

At the collection stage, the initial stage in the mobile forensics' method, what is being done is to search, collect and document evidence [31, 32, 33]. For testing the research that became the sample of the evidence analyzed was in the form of two smartphones which were screened as evidence in a crime case. Both smartphones are not rooted with the condition that the password security feature is active and the screen security is active. At this stage, documentation of matters relating to the smartphone is carried out. The specifications for evidence are listed in Table 2.

In addition to collecting and documenting, preparation and planning are also carried out on how the smartphone will be analyzed and what tools and tools are needed to support the process. In the design of the framework flow for analyzing smartphones to get digital artefacts related to the WhatsApp application in the condition of both smartphones that are not rooted with active screen security features. The workflow complies with forensic rules by taking steps that minimally alter the evidence.

For testing, an Android Smartphone is used in an unrooted state where some of its features have been disabled to prevent the user from damaging the operating system. The rooted state can remove these limitations so that full access to the system is allowed. For the condition of a rooted Android phone, the user will have more control over the settings, features and performance so that the process of accessing system files for forensic analysis will be easier. However, for forensic procedures on unrooted Android phones, it is recommended to avoid rooting permanently because it is very risky to change the evidence and can cause data to be overwritten.

Table 2. Research Evidence

	MERK	SERIES	MODEL	ANDROID	VERSION	CONDITION
				OS	*WHATSAPP*	
HP1	Samsung	Galaxy Note 9	SM-N960F	10	2.22.3.75	unrooted

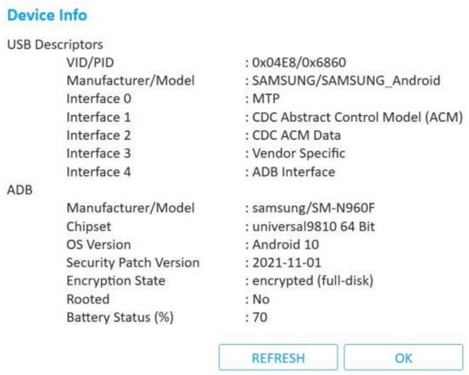
Examination Stages

At this stage, the acquisition and extraction process for internal and external memory from smartphone phones. Early Detection of Smartphones with Cellebrite UFED, as shown in Figure 3, using a console and a USB data cable. In carrying out the data collection process, the method used is an android backup and Android APK Downgrade backup. The tools used are MobilEdit, FinalData, and Cellebrite UFED. This process allows physical extraction by bypassing the decrypting bootloader (BTL) to make acquisitions with the android backup method using the Android Debug Bridge (ADB) as a command line tool in Cellebrite UFED that allows communicating with devices.

In Figure 4, it is explained that the acquisition and extraction process on Samsung smartphones is divided based on the chipset used, namely Qualcomm, Exynos and Generic chipsets. The Samsung Galaxy Note 9 smartphone uses the Exynos chipset. The adb command facilitates various device actions, such as installing and debugging applications. To use adb with devices connected via USB, USB debugging is enabled in the device's system settings, in the Developer options section. On Android 4.2 and up, the Developer options screen is hidden by default. To make it visible, go to Settings > About phone, then tap Version number seven times. Return to the previous screen to find the developer options at the bottom. Setting parameters on the smartphone before starting the acquisition and extraction process is done by ensuring that the display screen is always ON, the password, pin, and biometric are inactive, developer options are ON and USB setting is in data transfer condition.

Acquisition with an android backup method

To perform internal memory imaging on the two smartphones, researchers used the Cellebrite UFED tool, which will update the Android bootloader to retrieve data on the Android system partition and internal memory without having to root, and enable USB Debugging. The ongoing acquisition process is shown in Figure 5, which shows that the WhatsApp_backup.ab file is being acquired.



Device Info

USB Descriptors

VID/PID	: 0x04E8/0x6860
Manufacturer/Model	: SAMSUNG/SAMSUNG_Android
Interface 0	: MTP
Interface 1	: CDC Abstract Control Model (ACM)
Interface 2	: CDC ACM Data
Interface 3	: Vendor Specific
Interface 4	: ADB Interface

ADB

Manufacturer/Model	: samsung/SM-N960F
Chipset	: universal9810 64 Bit
OS Version	: Android 10
Security Patch Version	: 2021-11-01
Encryption State	: encrypted (full-disk)
Rooted	: No
Battery Status (%)	: 70

Figure 3. Device Information

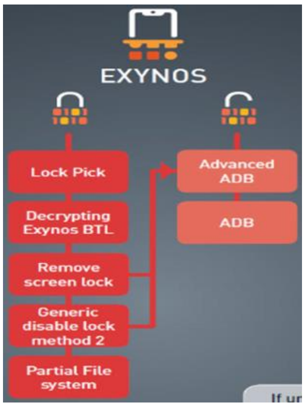
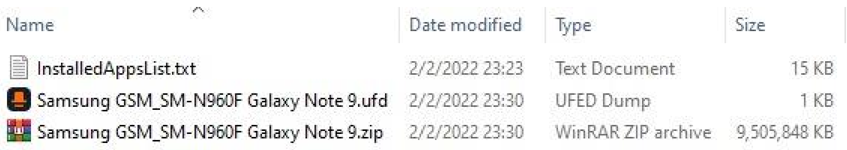


Figure 4. Acquisition and extraction process on android Samsung exynos



Name	Date modified	Type	Size
InstalledAppsList.txt	2/2/2022 23:23	Text Document	15 KB
Samsung GSM_SM-N960F Galaxy Note 9.ufd	2/2/2022 23:30	UFED Dump	1 KB
Samsung GSM_SM-N960F Galaxy Note 9.zip	2/2/2022 23:30	WinRAR ZIP archive	9,505,848 KB

Figure 5. File list acquisition result of Android backup method

The acquisition results in Figure 5 show that three files were acquired using the Android backup method. file with the type UFED Dump with a size of 9,505.848 KB will be extracted using the Cellebrite Physical Analyzer for later analysis of its artefacts.

Acquisition with Android APK Downgrade backup method

The acquisition process is carried out by first lowering the WhatsApp APK version to the standard version where the encrypted database file from WhatsApp can be decrypted and then the backup process is carried out. The APK version of WhatsApp installed on the smartphone will be saved in anticipation of failure during acquisition. Figure 6 shows that the WhatsApp apk is temporarily downgraded and the WhatsApp version installed (2.22.3.75) on the smartphone is stored on the Cellebrite device as a backup apk which can be downloaded for needs if there are problems during the acquisition process.

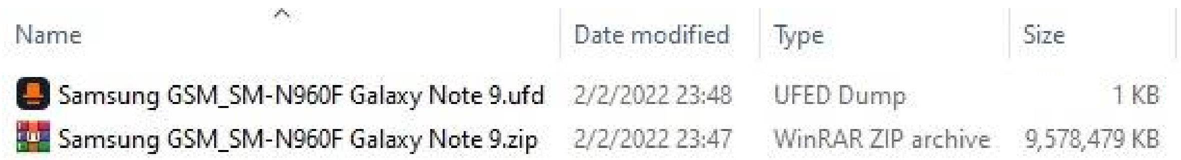
The acquisition results in Figure 6 show that two files were acquired using the Android APK Downgrade backup method. file with the type UFED Dump with a size of 9,578,479 KB which will be extracted using the Cellebrite Physical Analyzer for later analysis of the artifacts contained in it. the dump file is larger than the file acquired by the android backup method.

Extract WhatsApp Data from Image Data

The steps to extract data from the image are to take data from the external and internal memory backup images for the target smartphone. The data is stored in a folder labelled according to the backup date. The data sought is a dump file resulting from the acquisition process, as shown in Figure 5 dan Figure 6, which is then extracted. The extract results were analyzed to export the WhatsApp folder and the com.WhatsApp folder. To decrypt the encrypted database using the Cellebrite Physical Analyzer application, some artefacts can be seen in Hex View. The whole process is carried out by a hashing mechanism to maintain the integrity of the digital data. Figures 7 show the hash value using the SHA 256 algorithm for files acquired using the android backup method and the Android backup APK downgrade method.

The results of the acquisition and extraction with the Android backup method cannot see the contents of WhatsApp communications on smartphones due to the ability of the tools that can only describe the WhatsApp database up to a certain version that the mobile forensics device can decrypt [34, 35, 36, 37].

Figure 8 described that this research was carried out using the acquisition method by downgrading the application version where WhatsApp installed on the smartphone (version 2.22.3.75).



Name	Date modified	Type	Size
Samsung GSM_SM-N960F Galaxy Note 9.ufd	2/2/2022 23:48	UFED Dump	1 KB
Samsung GSM_SM-N960F Galaxy Note 9.zip	2/2/2022 23:47	WinRAR ZIP archive	9,578,479 KB

Figure 6. File list acquisition result of Android Backup APK Downgrade method

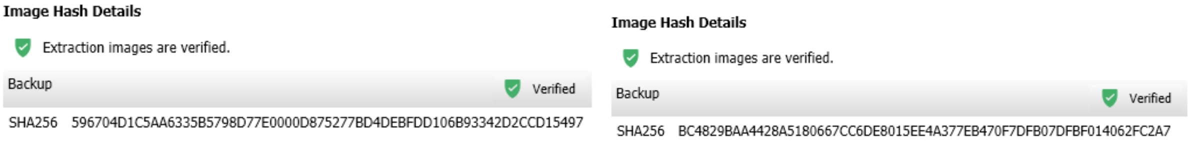


Image Hash Details

Extraction images are verified.

Backup — Verified

SHA256 596704D1C5AA6335B5798D77E0000D875277BD4DEBFDD106B93342D2CCD15497

Image Hash Details

Extraction images are verified.

Backup — Verified

SHA256 BC4829BAA4428A5180667CC6DE8015EE4A377EB470F7DFB07DFBF014062FC2A7

Figure 7. The acquisition hash value of android backup method and APK Downgrade

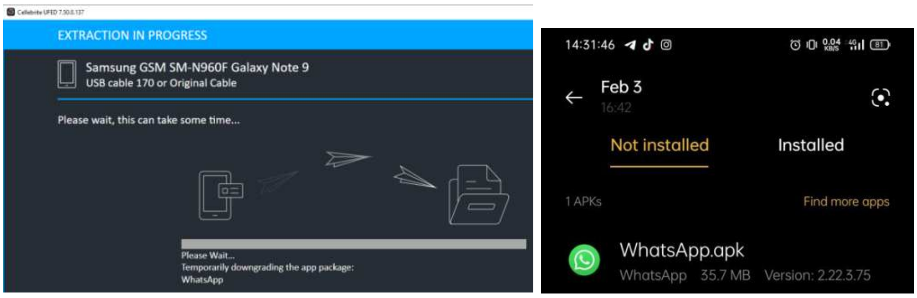
Figures 9 explained that the extraction file category is data content that can be extracted for further analysis according to the needs of digital evidence investigations. There is a clear difference in the extraction results of the two methods, where chat content is only found in the Android Backup APK Downgrade method.

Analysis Stages

This stage aims to uncover and analyze the results of the acquisition stage to obtain data related to the WhatsApp application. In this study, the Cellebrite Physical Analyzer tool is used to analyze the imaging results that have been carried out previously.

Call Log

Figure 10 shows that by analyzing the artefacts in the call log category, you will see the caller, recipient, timestamp, duration, status and source of file information extracted from the WhatsApp database msgstore.db.



Cellebrite UFED 7.50.0.137

EXTRACTION IN PROGRESS

Samsung GSM SM-N960F Galaxy Note 9
USB cable 170 or Original Cable

Please wait, this can take some time...

Please Wait...
Temporarily downgrading the app package:
WhatsApp

14:31:46

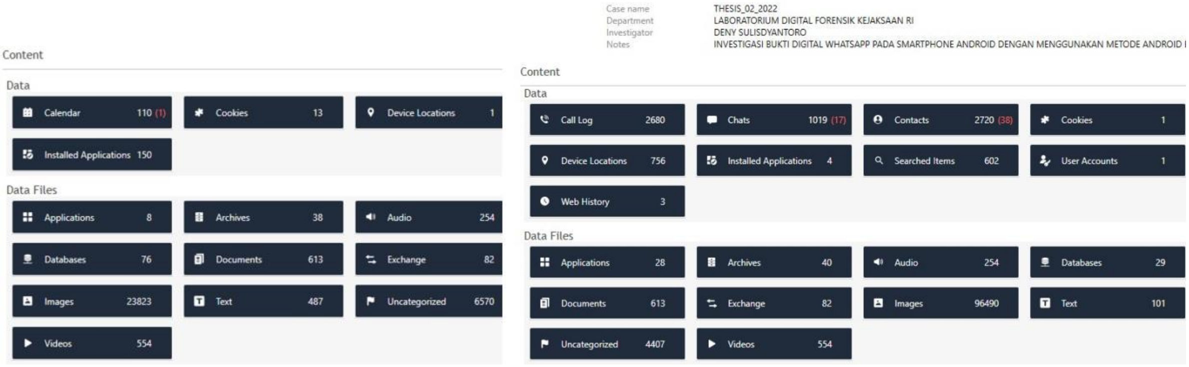
Feb 3
16:42

Not installed Installed

1 APKs Find more apps

WhatsApp.apk
WhatsApp 35.7 MB Version: 2.22.3.75

Figure 8. WhatsApp APK downgrading process



Content

Data

Calendar 110 (1)
Cookies 13
Device Locations 1
Installed Applications 150

Data Files

Applications 8
Archives 38
Audio 254
Databases 76
Documents 613
Exchange 82
Images 23823
Text 487
Uncategorized 6570
Videos 554

Case name THESIS_02_2022
Department LABORATORIUM DIGITAL FORENSIK KEJAKSAAN RI
Investigator DENY SULISDYANTORO
Notes INVESTIGASI BUKTI DIGITAL WHATSAPP PADA SMARTPHONE ANDROID DENGAN MENGGUNAKAN METODE ANDROID I

Content

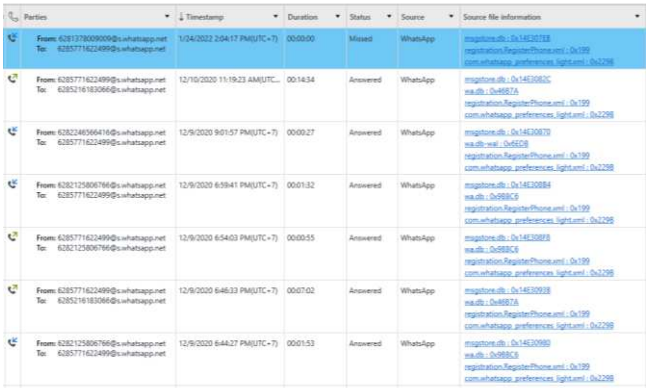
Data

Call Log 2680
Chats 1019 (17)
Contacts 2720 (38)
Cookies 1
Device Locations 756
Installed Applications 4
Searched Items 602
User Accounts 1
Web History 3

Data Files

Applications 28
Archives 40
Audio 254
Databases 29
Documents 613
Exchange 82
Images 96490
Text 101
Uncategorized 4407
Videos 554

Figure 9. Acquisition results with an android backup method and APK downgrade



Parties	Timestamp	Duration	Status	Source	Source file information
From: 6281378009009@s.whatsapp.net To: 6285771622499@s.whatsapp.net	1/24/2022 2:04:17 PM(UTC+7)	00:00:00	Missed	WhatsApp	msgstore.db : 0x14E307E8 registration.RegisterPhone.xml : 0x199 com.whatsapp_preferences_light.xml : 0x2298
From: 6285771622499@s.whatsapp.net To: 6285216183066@s.whatsapp.net	12/10/2020 11:19:23 AM(UTC...	00:14:34	Answered	WhatsApp	msgstore.db : 0x14E3082C wa.db : 0x4687A registration.RegisterPhone.xml : 0x199 com.whatsapp_preferences_light.xml : 0x2298
From: 6282246566416@s.whatsapp.net To: 6285771622499@s.whatsapp.net	12/9/2020 9:01:57 PM(UTC+7)	00:00:27	Answered	WhatsApp	msgstore.db : 0x14E30870 wa.db-wal : 0x6ED8 registration.RegisterPhone.xml : 0x199 com.whatsapp_preferences_light.xml : 0x2298
From: 6282125806766@s.whatsapp.net To: 6285771622499@s.whatsapp.net	12/9/2020 6:59:41 PM(UTC+7)	00:01:32	Answered	WhatsApp	msgstore.db : 0x14E30884 wa.db : 0x988C6 registration.RegisterPhone.xml : 0x199 com.whatsapp_preferences_light.xml : 0x2298
From: 6285771622499@s.whatsapp.net To: 6282125806766@s.whatsapp.net	12/9/2020 6:54:03 PM(UTC+7)	00:00:55	Answered	WhatsApp	msgstore.db : 0x14E308F8 wa.db : 0x988C6 registration.RegisterPhone.xml : 0x199 com.whatsapp_preferences_light.xml : 0x2298
From: 6285771622499@s.whatsapp.net To: 6285216183066@s.whatsapp.net	12/9/2020 6:46:33 PM(UTC+7)	00:07:02	Answered	WhatsApp	msgstore.db : 0x14E30938 wa.db : 0x4687A registration.RegisterPhone.xml : 0x199 com.whatsapp_preferences_light.xml : 0x2298
From: 6282125806766@s.whatsapp.net To: 6285771622499@s.whatsapp.net	12/9/2020 6:44:27 PM(UTC+7)	00:01:53	Answered	WhatsApp	msgstore.db : 0x14E30980 wa.db : 0x988C6 registration.RegisterPhone.xml : 0x199 com.whatsapp_preferences_light.xml : 0x2298

Figure 10. Data Analysis on Call Log Category

Chats

Figure 11 shows that by analyzing the artefacts in the chats category, participants, timestamp, last activity, and source of file information extracted from the WhatsApp msgstore.db database will be seen.

Contacts

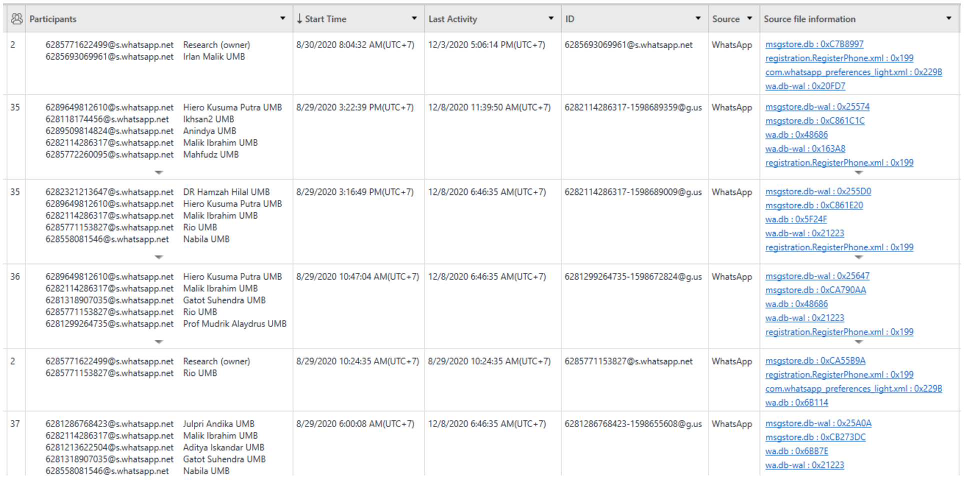
Figure 12 shows that by analyzing the artefacts in the contacts category, names, phone numbers, e-mail, participants, notes, sources, accounts and sources of file information extracted from the WhatsApp database msgstore.db are shown.

Device Locations

Figure 13 shows that by analyzing the artefacts in the device locations category, timestamps, address GPS coordinates, and file information sources are extracted from the WhatsApp database msgstore.db.

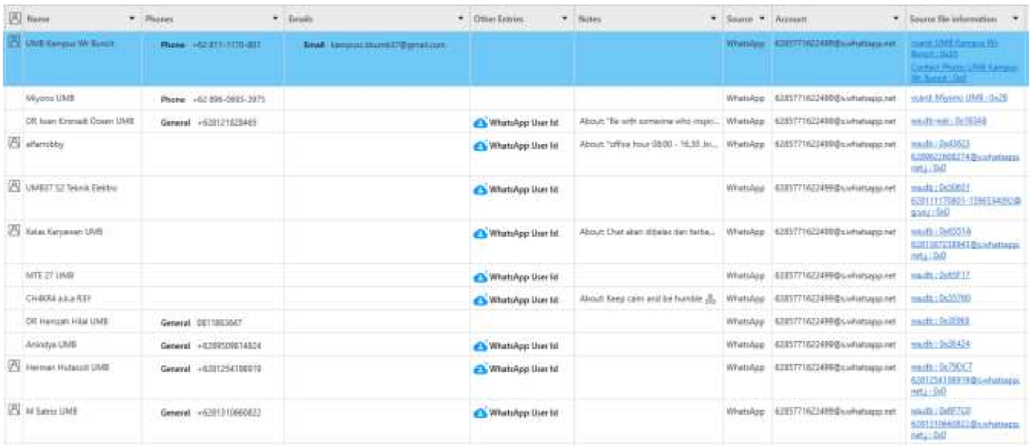
Web History

In Figure 14, it is shown that with the analysis of artefacts in the web history category, when was the last time the url was accessed, and the source of the file information extracted from the WhatsApp database msgstore.db.



	Participants		↓ Start Time	Last Activity	ID	Source	Source file information
2	6285771622499@s.whatsapp.net 6285693069961@s.whatsapp.net	Research (owner) Irlan Malik UMB	8/30/2020 8:04:32 AM(UTC+7)	12/3/2020 5:06:14 PM(UTC+7)	6285693069961@s.whatsapp.net	WhatsApp	msgstore.db : 0xC7B8997 registration.RegisterPhone.xml : 0x199 com.whatsapp_preferences_light.xml : 0x229B wa.db-wal : 0x20FD7
35	6289649812610@s.whatsapp.net 628118174456@s.whatsapp.net 6289509814824@s.whatsapp.net 6282114286317@s.whatsapp.net 6285772260095@s.whatsapp.net	Hiero Kusuma Putra UMB Ikhsan2 UMB Anindya UMB Malik Ibrahim UMB Mahfudz UMB	8/29/2020 3:22:39 PM(UTC+7)	12/8/2020 11:39:50 AM(UTC+7)	6282114286317-1598689359@g.us	WhatsApp	msgstore.db-wal : 0x25574 msgstore.db : 0xC861C1C wa.db : 0x48686 wa.db-wal : 0x163A8 registration.RegisterPhone.xml : 0x199
35	6282321213647@s.whatsapp.net 6289649812610@s.whatsapp.net 6282114286317@s.whatsapp.net 6285771153827@s.whatsapp.net 628558081546@s.whatsapp.net	DR Hamzah Hilal UMB Hiero Kusuma Putra UMB Malik Ibrahim UMB Rio UMB Nabila UMB	8/29/2020 3:16:49 PM(UTC+7)	12/8/2020 6:46:35 AM(UTC+7)	6282114286317-1598689009@g.us	WhatsApp	msgstore.db-wal : 0x255D0 msgstore.db : 0xC861E20 wa.db : 0x5F24F wa.db-wal : 0x21223 registration.RegisterPhone.xml : 0x199
36	6289649812610@s.whatsapp.net 6282114286317@s.whatsapp.net 6281318907035@s.whatsapp.net 6285771153827@s.whatsapp.net 6281299264735@s.whatsapp.net	Hiero Kusuma Putra UMB Malik Ibrahim UMB Gatot Suhendra UMB Rio UMB Prof Mudrik Alaydrus UMB	8/29/2020 10:47:04 AM(UTC+7)	12/8/2020 6:46:35 AM(UTC+7)	6281299264735-1598672824@g.us	WhatsApp	msgstore.db-wal : 0x25647 msgstore.db : 0xCA790AA wa.db : 0x48686 wa.db-wal : 0x21223 registration.RegisterPhone.xml : 0x199
2	6285771622499@s.whatsapp.net 6285771153827@s.whatsapp.net	Research (owner) Rio UMB	8/29/2020 10:24:35 AM(UTC+7)	8/29/2020 10:24:35 AM(UTC+7)	6285771153827@s.whatsapp.net	WhatsApp	msgstore.db : 0xCA55B9A registration.RegisterPhone.xml : 0x199 com.whatsapp_preferences_light.xml : 0x229B wa.db : 0x6B114
37	6281286768423@s.whatsapp.net 6282114286317@s.whatsapp.net 6281213622504@s.whatsapp.net 6281318907035@s.whatsapp.net 628558081546@s.whatsapp.net	Julpri Andika UMB Malik Ibrahim UMB Aditya Iskandar UMB Gatot Suhendra UMB Nabila UMB	8/29/2020 6:00:08 AM(UTC+7)	12/8/2020 6:46:35 AM(UTC+7)	6281286768423-1598655608@g.us	WhatsApp	msgstore.db-wal : 0x25A0A msgstore.db : 0xCB273DC wa.db : 0x6BB7E wa.db-wal : 0x21223

Figure 11. Data Analysis on Chats Category



Name	Phones	Emails	Other Entries	Notes	Source	Account	Source file information
UMB Kampus Wr Bunit	Phone +62 811-1170-811	Email [illegible]			WhatsApp	6285771622499@s.whatsapp.net	vcard: UMB Kampus Wr Bunit : 0x25 Contact Photo: UMB Kampus Wr Bunit : 0x0
Miyono UMB	Phone +62 896-0693-3975				WhatsApp	6285771622499@s.whatsapp.net	vcard: Miyono UMB : 0x28
DR Iwan Krisnadi Dosen UMB	General +6281211828465		WhatsApp User Id	About: "Be with someone who inspi...	WhatsApp	6285771622499@s.whatsapp.net	wa.db-wal : 0x16048
alfarrobby			WhatsApp User Id	About: "office hour 08:00 - 16.30 Ju...	WhatsApp	6285771622499@s.whatsapp.net	wa.db : 0x43623 6289622808274@s.whatsapp.net : 0x0
UMB27 S2 Teknik Elektro			WhatsApp User Id		WhatsApp	6285771622499@s.whatsapp.net	wa.db : 0x50611 6281111170801-1596134050@g.us : 0x0
Kelas Karyawan UMB			WhatsApp User Id	About: Chat akan dibalas dan terba...	WhatsApp	6285771622499@s.whatsapp.net	wa.db : 0x60016 6281387238843@s.whatsapp.net : 0x0
MTE 27 UMB			WhatsApp User Id		WhatsApp	6285771622499@s.whatsapp.net	wa.db : 0x65F17
CHAKRA a.k.a R3P			WhatsApp User Id	About: Keep calm and be humble	WhatsApp	6285771622499@s.whatsapp.net	wa.db : 0x55700
DR Hamzah Hilal UMB	General 0811883667				WhatsApp	6285771622499@s.whatsapp.net	wa.db : 0x28969
Anindya UMB	General +6289509814824		WhatsApp User Id		WhatsApp	6285771622499@s.whatsapp.net	wa.db : 0x38434
Herman Hutasoit UMB	General +6281254188919		WhatsApp User Id		WhatsApp	6285771622499@s.whatsapp.net	wa.db : 0x79DC7 6281254188919@s.whatsapp.net : 0x0
M Satria UMB	General +6281310660822		WhatsApp User Id		WhatsApp	6285771622499@s.whatsapp.net	wa.db : 0x6F7C0 6281310660822@s.whatsapp.net : 0x0

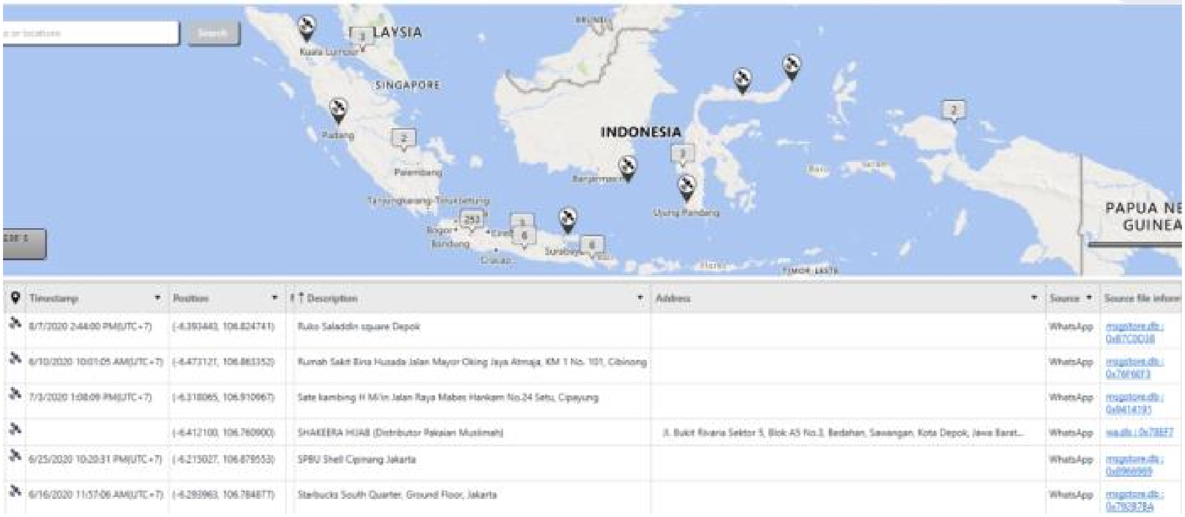
Figure 12. Data Analysis in Contacts Category

Audio

Figure 15 shows that the artefact analysis in the audio category will show file names, storage locations, file sizes, modified timestamps and file information sources extracted from WhatsApp data.

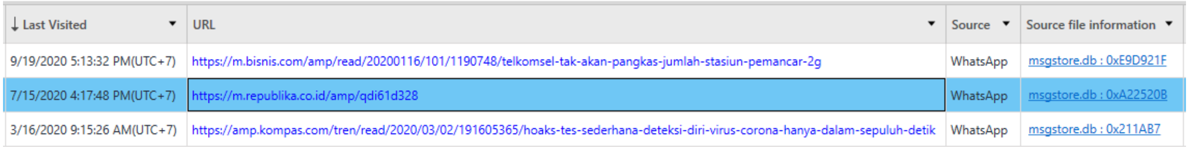
Databases

Figure 16 shows that the analysis of artefacts in the databases category will show file names, storage locations, file sizes, timestamps and file information sources extracted from WhatsApp data. It is also seen that the encrypted WhatsApp database can be decrypted by the Cellebrite tool so that artifacts can be displayed for further analysis and search according to digital evidence needs.



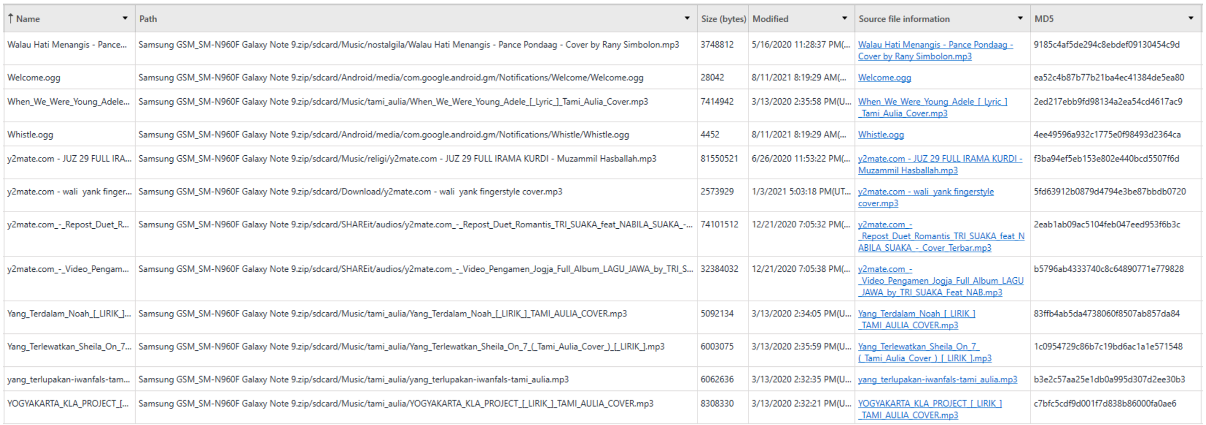
	Timestamp	Position	Description	Address	Source	Source file information
	8/7/2020 2:44:00 PM(UTC+7)	(-6.393443, 106.824741)	Ruko Saladdin square Depok		WhatsApp	msgstore.db : 0x87C0D18
	6/10/2020 10:01:05 AM(UTC+7)	(-6.473121, 106.863352)	Rumah Sakit Bina Husada Jalan Mayor Oking Jaya Atmaja, KM 1 No. 101, Cibinong		WhatsApp	msgstore.db : 0x76F6073
	7/3/2020 1:08:09 PM(UTC+7)	(-6.318065, 106.910967)	Sate kambing H M'in Jalan Raya Mabes Hankam No.24 Setu, Cipayung		WhatsApp	msgstore.db : 0x9414781
		(-6.412100, 106.760900)	SHAKEERA HIJAB (Distributor Pakaian Muslimah)	Jl. Bukit Rivaria Sektor 5, Blok A5 No.3, Bedahan, Sawangan, Kota Depok, Jawa Barat...	WhatsApp	wa.db : 0x78EF7
	6/25/2020 10:20:31 PM(UTC+7)	(-6.215027, 106.879553)	SPBU Shell Cipinang Jakarta		WhatsApp	msgstore.db : 0x8966969
	6/16/2020 11:57:06 AM(UTC+7)	(-6.293963, 106.784877)	Starbucks South Quarter, Ground Floor, Jakarta		WhatsApp	msgstore.db : 0x7828784

Figure 13. Data Analysis in Device Locations Category



Last Visited	URL	Source	Source file information
9/19/2020 5:13:32 PM(UTC+7)	https://m.bisnis.com/amp/read/20200116/101/1190748/telkomsel-tak-akan-pangkas-jumlah-stasiun-pemancar-2g	WhatsApp	msgstore.db : 0xE9D921F
7/15/2020 4:17:48 PM(UTC+7)	https://m.republika.co.id/amp/qdi61d328	WhatsApp	msgstore.db : 0xA22520B
3/16/2020 9:15:26 AM(UTC+7)	https://amp.kompas.com/tren/read/2020/03/02/191605365/hoaks-tes-sederhana-deteksi-diri-virus-corona-hanya-dalam-sepuluh-detik	WhatsApp	msgstore.db : 0x211AB7

Figure 14. Data Analysis in the Web History category



Name	Path	Size (bytes)	Modified	Source file information	MD5
Walau Hati Menangis - Pance...	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Music/nostalgila/Walau Hati Menangis - Pance Pondaag - Cover by Rany Simbolon.mp3	3748812	5/16/2020 11:28:37 PM(...	Walau Hati Menangis - Pance Pondaag - Cover by Rany Simbolon.mp3	9185c4af5de294c8ebdef09130454c9d
Welcome.ogg	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Android/media/com.google.android.gm/Notifications/Welcome/Welcome.ogg	28042	8/11/2021 8:19:29 AM(...	Welcome.ogg	ea52c4b87b77b21ba4ec41384de5ea80
When_We_Were_Young_Adele...	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Music/tami_aulia/When_We_Were_Young_Adele_[_Lyric_]_Tami_Aulia_Cover.mp3	7414942	3/13/2020 2:35:58 PM(U...	When_We_Were_Young_Adele_[_Lyric_]_Tami_Aulia_Cover.mp3	2ed217ebb9fd98134a2ea54cd4617ac9
Whistle.ogg	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Android/media/com.google.android.gm/Notifications/Whistle/Whistle.ogg	4452	8/11/2021 8:19:29 AM(...	Whistle.ogg	4ee49596a932c1775e0f98493d2364ca
y2mate.com - JUZ 29 FULL IRA...	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Music/religi/y2mate.com - JUZ 29 FULL IRAMA KURDI - Muzammil Hasballah.mp3	81550521	6/26/2020 11:53:22 PM(...	y2mate.com - JUZ 29 FULL IRAMA KURDI - Muzammil Hasballah.mp3	f3ba94ef5eb153e802e440bcd5507f6d
y2mate.com - wali yank finger...	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Download/y2mate.com - wali yank fingerstyle cover.mp3	2573929	1/3/2021 5:03:18 PM(UT...	y2mate.com - wali_yank fingerstyle cover.mp3	5fd63912b0879d4794e3be87bbdb0720
y2mate.com_-_Repost_Duet_R...	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/SHAREit/audios/y2mate.com_-_Repost_Duet_Romantis_TRI_SUAKA_feat_NABILA_SUAKA_-...	74101512	12/21/2020 7:05:32 PM(...	y2mate.com_-_Repost_Duet_Romantis_TRI_SUAKA_feat_NABILA_SUAKA_-_Cover_Terbar.mp3	2eab1ab09ac5104feb047eed953f6b3c
y2mate.com_-_Video_Pengam...	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/SHAREit/audios/y2mate.com_-_Video_Pengamen_Jogja_Full_Album_LAGU_JAWA_by_TRI_S...	32384032	12/21/2020 7:05:38 PM(...	y2mate.com_-_Video_Pengamen_Jogja_Full_Album_LAGU_JAWA_by_TRI_SUAKA_Feat_NAB.mp3	b5796ab4333740c8c64890771e779828
Yang_Terdalam_Noah_[_LIRIK_]...	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Music/tami_aulia/Yang_Terdalam_Noah_[_LIRIK_]_TAMI_AULIA_COVER.mp3	5092134	3/13/2020 2:34:05 PM(U...	Yang_Terdalam_Noah_[_LIRIK_]_TAMI_AULIA_COVER.mp3	83ffb4ab5da4738060f8507ab857da84
Yang_Terlewatkan_Sheila_On_7...	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Music/tami_aulia/Yang_Terlewatkan_Sheila_On_7_(_Tami_Aulia_Cover_)_[_LIRIK_].mp3	6003075	3/13/2020 2:35:59 PM(U...	Yang_Terlewatkan_Sheila_On_7_(_Tami_Aulia_Cover_)_[_LIRIK_].mp3	1c0954729c86b7c19bd6ac1a1e571548
yang_terlupakan-iwanfals-tam...	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Music/tami_aulia/yang_terlupakan-iwanfals-tami_aulia.mp3	6062636	3/13/2020 2:32:35 PM(U...	yang_terlupakan-iwanfals-tami_aulia.mp3	b3e2c57aa25e1db0a995d307d2ee30b3
YOGYAKARTA_KLA_PROJECT_[...	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Music/tami_aulia/YOGYAKARTA_KLA_PROJECT_[_LIRIK_]_TAMI_AULIA_COVER.mp3	8308330	3/13/2020 2:32:21 PM(U...	YOGYAKARTA_KLA_PROJECT_[_LIRIK_]_TAMI_AULIA_COVER.mp3	c7bfc5cdf9d001f7d838b86000fa0ae6

Figure 15. Data Analysis in Audio category

Documents

Figure 17 shows that the analysis of artefacts in the documents category will show file names, storage locations, file sizes, timestamps and file information sources extracted from internal and external memory on smartphones.

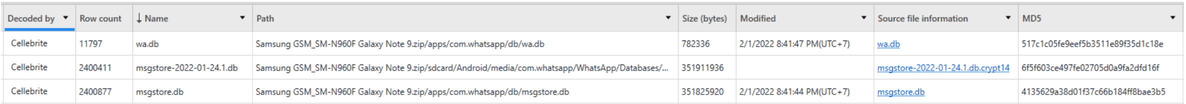
Images

In Figure 18, it is shown that the analysis of artefacts in the images category will show file names, storage locations, file sizes, timestamps, image senders and file information sources extracted from the WhatsApp database and the smartphone's internal/external memory.

Videos

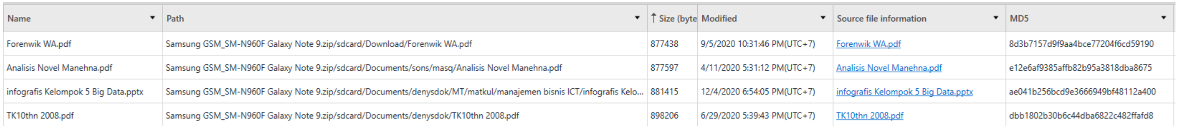
Figure 19 shows that the analysis of artefacts in the videos category will show file names, storage locations, file sizes, timestamps, image senders and file information sources extracted from the WhatsApp database and smartphone internal/external memory.

From the results of the acquisition and extraction above, this study provides an overview of how to carry out acquisition, extraction and forensic analysis of artefacts in the Android-based WhatsApp application to obtain forensic evidence information related to data that shows details of file names, file locations, file sizes, GPS locations, and data related to other investigation needs.



Decoded by	Row count	↓ Name	Path	Size (bytes)	Modified	Source file information	MD5
Cellebrite	11797	wa.db	Samsung GSM_SM-N960F Galaxy Note 9.zip/apps/com.whatsapp/db/wa.db	782336	2/1/2022 8:41:47 PM(UTC+7)	wa.db	517c1c05fe9eef5b3511e89f35d1c18e
Cellebrite	2400411	msgstore-2022-01-24.1.db	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Android/media/com.whatsapp/WhatsApp/Databases/...	351911936		msgstore-2022-01-24.1.db.crypt14	6f5f603ce497fe02705d0a9fa2dfd16f
Cellebrite	2400877	msgstore.db	Samsung GSM_SM-N960F Galaxy Note 9.zip/apps/com.whatsapp/db/msgstore.db	351825920	2/1/2022 8:41:44 PM(UTC+7)	msgstore.db	4135629a38d01f37c66b184ff8bae3b5

Figure 16. Data Analysis in the Databases category



Name	Path	↑ Size (byte	Modified	Source file information	MD5
Forenwik WA.pdf	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Download/Forenwik WA.pdf	877438	9/5/2020 10:31:46 PM(UTC+7)	Forenwik WA.pdf	8d3b7157d9f9aa4bce77204f6cd59190
Analisis Novel Manehna.pdf	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Documents/sons/masq/Analisis Novel Manehna.pdf	877597	4/11/2020 5:31:12 PM(UTC+7)	Analisis Novel Manehna.pdf	e12e6af9385affb82b95a3818dba8675
infografis Kelompok 5 Big Data.pptx	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Documents/denysdok/MT/matkul/manajemen bisnis ICT/infografis Kelo...	881415	12/4/2020 6:54:05 PM(UTC+7)	infografis Kelompok 5 Big Data.pptx	ae041b256bcd9e3666949bf48112a400
TK10thn 2008.pdf	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Documents/denysdok/TK10thn 2008.pdf	898206	6/29/2020 5:39:43 PM(UTC+7)	TK10thn 2008.pdf	dbb1802b30b6c44dba6822c482ffafd8

Figure 17. Data Analysis in the Documents category

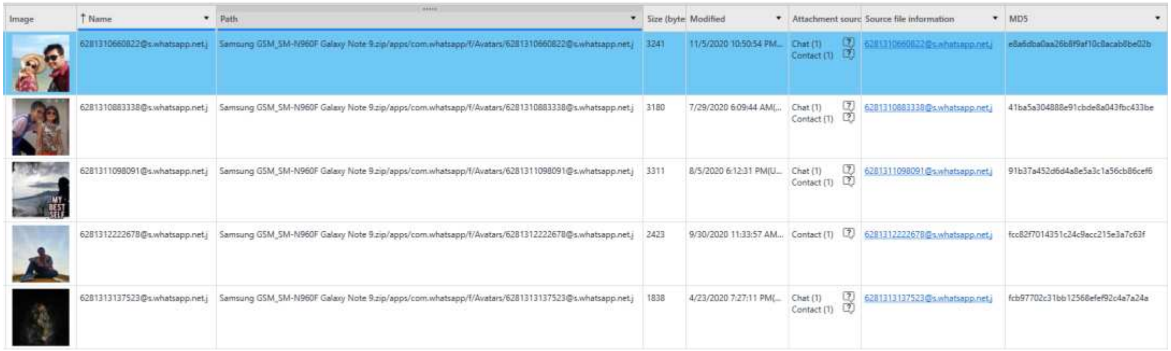
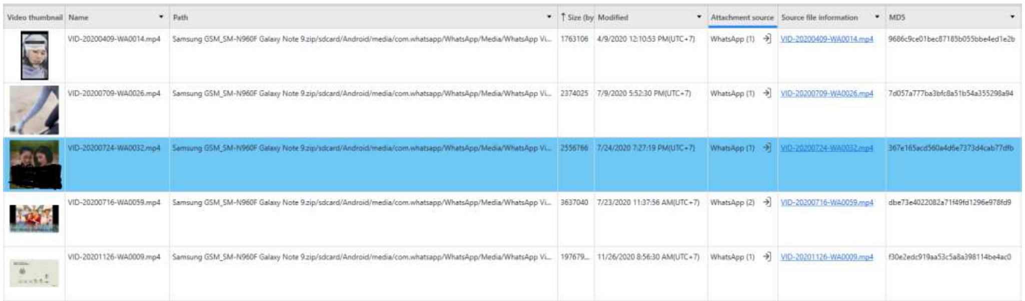


Image	↑ Name	Path	Size (byte	Modified	Attachment sourc	Source file information	MD5
	6281310660822@s.whatsapp.net.j	Samsung GSM_SM-N960F Galaxy Note 9.zip/apps/com.whatsapp/f/Avatars/6281310660822@s.whatsapp.net.j	3241	11/5/2020 10:50:54 PM...	Chat (1) Contact (1)	6281310660822@s.whatsapp.net.j	e8a6dba0aa26b8f9af10c8acab8be02b
	6281310883338@s.whatsapp.net.j	Samsung GSM_SM-N960F Galaxy Note 9.zip/apps/com.whatsapp/f/Avatars/6281310883338@s.whatsapp.net.j	3180	7/29/2020 6:09:44 AM(...	Chat (1) Contact (1)	6281310883338@s.whatsapp.net.j	41ba5a304888e91cbde8a043fbc433be
	6281311098091@s.whatsapp.net.j	Samsung GSM_SM-N960F Galaxy Note 9.zip/apps/com.whatsapp/f/Avatars/6281311098091@s.whatsapp.net.j	3311	8/5/2020 6:12:31 PM(U...	Chat (1) Contact (1)	6281311098091@s.whatsapp.net.j	91b37a452d6d4a8e5a3c1a56cb86cef6
	6281312222678@s.whatsapp.net.j	Samsung GSM_SM-N960F Galaxy Note 9.zip/apps/com.whatsapp/f/Avatars/6281312222678@s.whatsapp.net.j	2423	9/30/2020 11:33:57 AM...	Contact (1)	6281312222678@s.whatsapp.net.j	fcc82f7014351c24c9acc215e3a7c63f
	6281313137523@s.whatsapp.net.j	Samsung GSM_SM-N960F Galaxy Note 9.zip/apps/com.whatsapp/f/Avatars/6281313137523@s.whatsapp.net.j	1838	4/23/2020 7:27:11 PM(...	Chat (1) Contact (1)	6281313137523@s.whatsapp.net.j	fcb97702c31bb12568efef92c4a7a24a

Figure 18. Data Analysis in the Images category



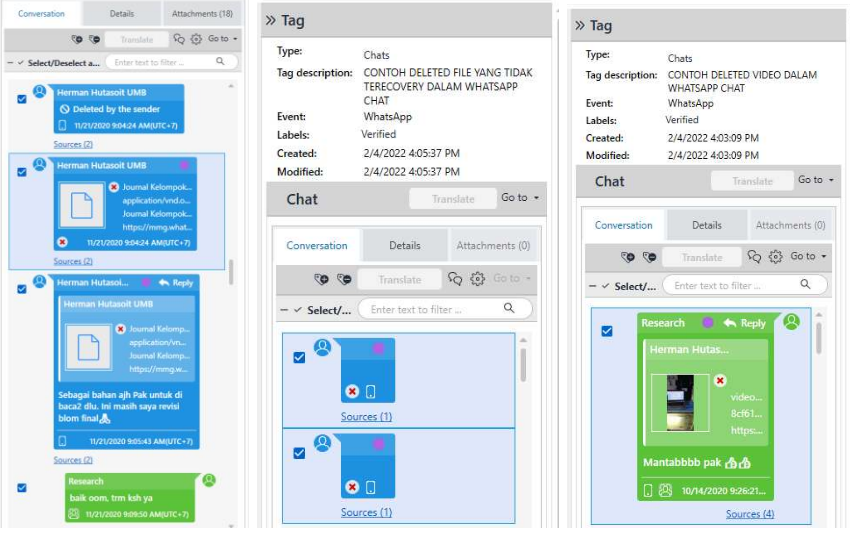
Video thumbnail	Name	Path	Size (by	Modified	Attachment source	Source file information	MD5
	VID-20200409-WA0014.mp4	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Android/media/com.whatsapp/WhatsApp/Media/WhatsApp Vi...	1763106	4/9/2020 12:10:53 PM(UTC+7)	WhatsApp (1)	VID-20200409-WA0014.mp4	9686c9ce01bec87185b055bbe4ed1e2b
	VID-20200709-WA0026.mp4	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Android/media/com.whatsapp/WhatsApp/Media/WhatsApp Vi...	2374025	7/9/2020 5:52:30 PM(UTC+7)	WhatsApp (1)	VID-20200709-WA0026.mp4	7d057a777ba3bfc8a51b54a355298a94
[redacted]	VID-20200724-WA0032.mp4	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Android/media/com.whatsapp/WhatsApp/Media/WhatsApp Vi...	2556766	7/24/2020 7:27:19 PM(UTC+7)	WhatsApp (1)	VID-20200724-WA0032.mp4	367e165acd560a4d6e7373d4cab77dfb
	VID-20200716-WA0059.mp4	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Android/media/com.whatsapp/WhatsApp/Media/WhatsApp Vi...	3637040	7/23/2020 11:37:56 AM(UTC+7)	WhatsApp (2)	VID-20200716-WA0059.mp4	dbe73e4022082a71f49fd1296e978fd9
	VID-20201126-WA0009.mp4	Samsung GSM_SM-N960F Galaxy Note 9.zip/sdcard/Android/media/com.whatsapp/WhatsApp/Media/WhatsApp Vi...	197679...	11/26/2020 8:56:30 AM(UTC+7)	WhatsApp (1)	VID-20201126-WA0009.mp4	f30e2edc919aa53c5a8a398114be4ac0

Figure 19. Data Analysis on Videos category

It can be seen that the acquisition and extraction using the Android backup method cannot describe the encrypted WhatsApp database compared to the Android APK downgrade backup method proposed in this study. From the artefacts that have been analyzed, there are deleted files found in WhatsApp communication. For a cross, it means that the data is in a deleted condition where deleted files can be recovered or not. In the artefact analysis of the acquired file, there is a hash value with the MD5 algorithm, which guarantees the integrity of the data that is not the result of a modification, meaning that there is no change during the confiscation until the completion of the digital forensic process on the smartphone. Figure 20 shows that chat conversations are in the form of text that can be recovered, while for file attachments such as pdf documents, the video contained in the communication can be seen as thumbnails and file names.

Table 3 compares the acquisition and extraction results with the Cellebrite tools using the Android Backup and Android Backup APK Downgrade methods. In this study, acquisition and extraction were also carried out using MobilEdit and FinalData tools. Table 3 shows that the Android backup APK downgrade method can extract all categories of artifacts, especially the chat category except the calendar category and has the highest number of artefacts that can be extracted.

Table 4 shows the percentage of the number of artefacts compared to other methods. The table shows that the Android Backup APK Downgrade method can retrieve 651% more artefacts than the Android Backup Method, 851% more than the Logical-MobilEdit method and 854% more than the Android Backup Final Data method.



Herman Hutasoit UMB
Deleted by the sender
11/21/2020 9:04:24 AM(UTC+7)
Sources (2)

Herman Hutasoit UMB
Journal Kelompok...
application/vnd.o...
Journal Kelompok...
https://mmg.what...
11/21/2020 9:04:24 AM(UTC+7)
Sources (2)

Herman Hutasoi... Reply
Herman Hutasoit UMB
Journal Kelomp...
application/vn...
Journal Kelomp...
https://mmg.w...
Sebagai bahan ajh Pak untuk di baca2 dlu. Ini masih saya revisi blom final
11/21/2020 9:05:43 AM(UTC+7)
Sources (2)

Research
baik oom, trm ksh ya
11/21/2020 9:09:50 AM(UTC+7)

» Tag

Type: Chats
Tag description: CONTOH DELETED FILE YANG TIDAK TERECOVERY DALAM WHATSAPP CHAT
Event: WhatsApp
Labels: Verified
Created: 2/4/2022 4:05:37 PM
Modified: 2/4/2022 4:05:37 PM

» Tag

Type: Chats
Tag description: CONTOH DELETED VIDEO DALAM WHATSAPP CHAT
Event: WhatsApp
Labels: Verified
Created: 2/4/2022 4:03:09 PM
Modified: 2/4/2022 4:03:09 PM

Research Reply
Herman Hutas...
video...
8cf61...
https:...
Mantabbbb pak
10/14/2020 9:26:21...
Sources (4)

Figure 20. Deleted data

Table 3. Comparison of acquisition and extraction results

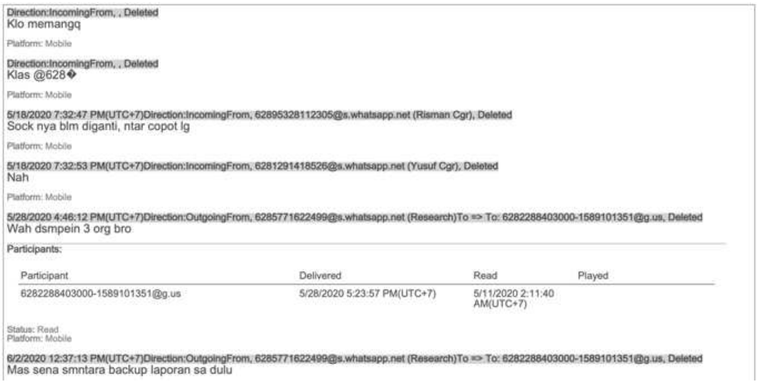
	Cellebrite		MobilEdit	FinalData
	METHODS			
	Android Backup	Android Backup APK Downgrade	Logical	Android Backup
Applications	8	28	0	0
Archives	37	39	0	0
Audio	251	251	268	268
Calendar	110	0	110	16
Call log	0	2676	154	154
Chat	0	1019	935 (SMS)	935 (SMS)
Contacts	0	2720	3680	3680
Cookies	13	1	0	0
*Database*s	70	28	0	0
Device Info	3	1	1	1
Documents	587	587	689	689
Exchange	82	82	0	0
Images	21100	38371	16986	16986
Installed Applications	150	4	463	463
Locations	1	746	0	0
Searched Items	0	602	0	0
Text	470	101	0	0
Timeline	696	146791	0	0
Uncategorized	6430	4333	0	0
User Accounts	0	1	0	0
Videos	545	545	1023	1023
Web History	0	3	0	0
Total	30553	198929	23374	23280

Table 4. Percentage of acquisition and extraction report

	Android Backup APK Downgrade Cellebrite	**Android Backup Cellebrite**	**Logical MobilEdit**	**Android Backup FinalData**
Android Backup APK Downgrade Cellebrite	100	**651,0948188**	851,0695645	854,5060137
Android Backup Cellebrite	15,35874609	100	130,7136134	131,2414089
Logical MobilEdit	76,50312572	11,74992083	100	100,4037801
Android Backup FinalData	76,19546362	11,70266779	99,59784376	100

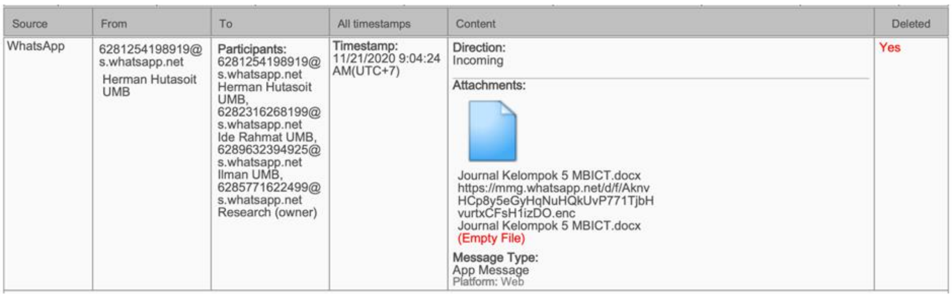
Deleted artefact

Recovery of deleted files/data in the WhatsApp application is an important thing that needs to be pursued in every mobile forensic action. The acquisition of WhatsApp digital evidence using the Android Backup APK Downgrade method can recover deleted data in WhatsApp text conversation communications, while for file attachments, only the thumbnail appears, as shown in Figure 21 and Figure 22.



```
Direction:IncomingFrom, , Deleted
Klo memangq
Platform: Mobile

Direction:IncomingFrom, , Deleted
Klas @628�
Platform: Mobile

5/18/2020 7:32:47 PM(UTC+7)Direction:IncomingFrom, 62895328112305@s.whatsapp.net (Risman Cgr), Deleted
Sock nya blm diganti, ntar copot lg
Platform: Mobile

5/18/2020 7:32:53 PM(UTC+7)Direction:IncomingFrom, 6281291418526@s.whatsapp.net (Yusuf Cgr), Deleted
Nah
Platform: Mobile

5/28/2020 4:46:12 PM(UTC+7)Direction:OutgoingFrom, 6285771622499@s.whatsapp.net (Research)To => To: 6282288403000-1589101351@g.us, Deleted
Wah dsmpein 3 org bro
Participants:

  Participant                      Delivered                     Read                Played
  6282288403000-1589101351@g.us    5/28/2020 5:23:57 PM(UTC+7)   5/11/2020 2:11:40
                                                                 AM(UTC+7)

Status: Read
Platform: Mobile

6/2/2020 12:37:13 PM(UTC+7)Direction:OutgoingFrom, 6285771622499@s.whatsapp.net (Research)To => To: 6282288403000-1589101351@g.us, Deleted
Mas sena smntara backup laporan sa dulu
```

Figure 21. WhatsApp text communication data recovery



Source	From	To	All timestamps	Content	Deleted
WhatsApp	6281254198919@ s.whatsapp.net Herman Hutasoit UMB	**Participants:** 6281254198919@ s.whatsapp.net Herman Hutasoit UMB, 6282316268199@ s.whatsapp.net Ide Rahmat UMB, 6289632394925@ s.whatsapp.net Ilman UMB, 6285771622499@ s.whatsapp.net Research (owner)	**Timestamp:** 11/21/2020 9:04:24 AM(UTC+7)	**Direction:** Incoming **Attachments:** Journal Kelompok 5 MBICT.docx https://mmg.whatsapp.net/d/f/Aknv HCp8y5eGyHqNuHQkUvP771TjbH vurtxCFsH1izDO.enc Journal Kelompok 5 MBICT.docx (Empty File) **Message Type:** App Message Platform: Web	Yes

Figure 22. Unrecovered WhatsApp communication document file

Figure 22 shows the sending of the document file “Jurnal Grup 5 MBICT.docx” in a WhatsApp group communication sent by Herman Hutasoit UMB (6281254198919), but the contents of the file cannot be extracted (empty file) and only the file name of the document can be known.

CONCLUSION

The procedural approach used to obtain WhatsApp artefact data on an Android smartphone can be in different ways depending on several things, such as the type of smartphone manufacturer, smartphone security features, the transfer protocol used, and the Android version. There is a hash value with the SHA256 algorithm on the results of the acquisition and extraction using the android backup method and the Android backup APK downgrade method, and there is a hash value with the MD5 algorithm on the artefacts of the acquisition and extraction files. The hash value guarantees the integrity of the data that is not the result of a modification, meaning that there is no change during the confiscation until the digital forensic process on electronic evidence is completed. With the steps of the forensic analysis procedure carried out in this study, we succeeded in obtaining evidence artefacts in the form of chat sessions, avatars, contact numbers on the WhatsApp application, voice notes, profile photos, the identity of the WhatsApp account owner and also being able to get other media files and most importantly database files. encrypted backups.

A common challenge for forensic investigators is the ever-evolving WhatsApp encryption standard to protect backups from unauthorized access. Therefore, it is very important for forensic investigators to always update technological developments related to WhatsApp backup databases to extract chat sessions that may exist on the suspect's device. Another challenge is that WhatsApp has added end-to-end encryption facility for all messages. Therefore, research is needed to conduct forensics on conversational sessions that utilize end-to-end encryption. The WhatsApp database is encrypted using crypt14 with WhatsApp technology which is continuously updated by the developer, so further research and testing need to be carried out regarding forensic procedures for the latest encryption features of the WhatsApp messaging application in the future. Given that the WhatsApp application is a cross-platform application, it is also important to conduct a forensic analysis of WhatsApp artefacts on other platforms.

REFERENCES

[1] NN, “Laporan Survei Internet APJII 2019 – 2020 Q2),” *Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)*, 2020.

[2] N. Anwar and I. Riadi, “Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web,” *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, vol. 3, no. 1, pp. 1-10, Jun. 2017, doi: 10.26555/jiteki.v3i1.6643.

[3] R. Umar, I. Riadi and G. M. Zamroni, “A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements,” *International Journal of Advanced Computer Science and Applications*, vol. 8, no, 12, pp. 69-75, 2017, doi: 10.14569/IJACSA.2017.081210

[4] R. Umar, I. Riadi, and B. F. Muthohirin, “Live forensics of tools on android devices for email forensics,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 17, no. 4, pp. 1803–1809, Aug. 2019, doi: 10.12928/TELKOMNIKA.v17i4.11748.

[5] NN, “Digital 2022 Global Overview Report,” *We are Social,* January 2022.

[6] T. D. Larasati, D. Bekti, and C. Hidayanto, “Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10,” *Seminar Nasional Sistem Informasi Indonesia*, 2017, pp. 245–255.

[7] NN, “*Jaksa Cecar Saksi Ahli Forensik soal Isi Grup WA ‘Deklarator KAMI’*,” 2021. https://news.detik.com/berita/d-5379468/jaksa-cecar-saksi-ahli-forensik-soal-isi-grup-wa-deklarator-kami (accessed Apr. 06, 2021).

[8] NN, “*Saksi Ahli Forensik Digital Bongkar Chat Ratna dengan Fadli dan Said Iqbal*,” 2019. https://www.jawapos.com/nasional/hukum-kriminal/25/04/2019/saksi-ahli-forensik-digital-bongkar-chat-ratna-dengan-fadli-dan-said-iqbal/ (accessed Apr. 06, 2021).

[9] H. Zhang, L. Chen and Q. Liu, "Digital Forensic Analysis of Instant Messaging Applications on Android Smartphones," *2018 International Conference on Computing, Networking and Communications (ICNC)*, Maui, HI, USA, 2018, pp. 647-651, doi: 10.1109/ICCNC.2018.8390330.

[10] R. Dinnur Rahman and I. Riadi, “Framework Analysis of IDFIF V2 in WhatsApp Investigation Process on Android Smartphones,” *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 3, pp. 213–222, 2019, doi: 10.17781/P002610.

[11] V. Arista Yuliani and I. Riadi, “Forensic Analysis WhatsApp Mobile Application on Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Framework,” *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 3, pp. 223–231, 2019, doi: 10.17781/P002615.

[12] P. Widiandana, I. Riadi, A. Dahlan Jl Soepomo, and J. Yogyakarta, “Analisis Investigasi Forensik Cyber Bullying pada Whatsapp Messenger Menggunakan Metode National Institute of Standards and Technology (NIST),” *Analisis Investigasi Forensik Cyber Bullying pada Whatsapp Messenger Menggunakan Metode National Institute of Standards and Technology (NIST)* , vol. 17, pp. 488–493, 2019.

[13] A. Marfianto, “WhatsApp Messenger Forensic Analysis Based on Android Using Text Mining Method,” *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 3, pp. 319–327, 2018, doi: 10.17781/P002470.

[14] I. Riadi and dan Muhamad Ermansyah Rauli, “Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics,” *Jurnal Teknik Elektro,* vol. 10, no. 1, pp. 18–22, 2018, doi: 10.15294/jte.v10i1.14070

[15] Y. Novaria Kunang and A. Khristian, “Implementasi Prosedur Forensik untuk Analisis Artefak Whatsapp pada Ponsel Android,” in *Annual Research Seminar 2016*, 2016, vol. 2, no. 1.

[16] I. Saputra and M. Nauval Azhar, “Analisis dan Investigasi Forensik Digital Live Memory Untuk Deteksi Tingkah Laku Agresi Pada Aplikasi Whatsapp,” *Seminar Nasional dan Diskusi Panel Multidisiplin Hasil Penelitian & Pengabdian kepada Masyarakat*, 2018, pp. 119–125.

[17] A. Wirara, B. Hardiawan, M. Salman, and B. Siber dan Sandi Negara, “Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan ‘WhatsApp,’” *Teknoin*, vol. 26, no. 1, pp. 66–74, 2020.

[18] N. Anggraini, S. U. Masruroh, and H. Tiaraningtias, “Analisa Forensik Whatsapp Messanger Pada Smartphone Android,” *Jurnal Ilmiah FIFO*, vol. 12, no. 1, pp. 83-100, Jul. 2020, doi: 10.22441/fifo.2020.v12i1.008.

[19] Z. Akbar, B. Nugraha, and M. Alaydrus, "Whatsapp Forensics Pada Android Smartphone: A Survey," *SINERGI*, vol. 20, no. 3, pp. 207–212, Dec. 2016, doi: 10.22441/sinergi.2016.3.006.

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

[21] H. A. Ghannam, "Forensic Analysis of Artifacts of Giant Instant Messaging 'WhatsApp' in Android Smartphone," *Journal of Applied Information, Communication and Technology*, vol. 5, no. 2, pp. 63–72, Oct. 2018, doi: 10.33555/ejaict.v5i2.55.

[22] I. Riadi, R. Umar and A. Firdonsyah, "Identification of Digital Evidence on Android's Blackberry Messenger Using NIST Mobile Forensic Method," *International Journal of Computer Science and Information Security*, vol. 15, no. 5, pp. 155–160, May 2017.

[23] M. N. Al-Azhar, *Digital Forensic - Panduan Praktis Investigasi Komputer*. Salemba Infotek, 2012.

[24] DAC Janet Williams QPM, "ACPO Good Practice Guide for Digital Evidence," 2012.

[25] M. N. Al-Azhar, *Seri 1 Digital Forensik - Panduan Umum Digital Forensik Pada Platform Windows, Linux, Mac & Mobile*. Salemba Infotek, 2021.

[26] S. Al Hidaifi, "Mobile Forensics: Android Platforms and WhatsApp Extraction Tools," *International Journal of Computer Applications*, vol. 179, no. 47, pp. 25–29, Jun. 2018, doi: 10.5120/ijca2018917264.

[27] 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, pp. 69–75, 2017, doi: 10.14569/ijacsa.2017.081210.

[28] M. I. Ramadhan and I. Riadi, "Forensic WhatsApp based Android using National Institute of Standard Technology (NIST) Method," *International Journal of Computer Applications*, vol. 177, no. 8, pp. 975–8887, 2019, doi: 10.13140/RG.2.2.24072.78088.

[29] H. Trisnasenjaya, "Forensic Analysis of Android-based WhatsApp Messenger Against Fraud Crime Using the National Institute of Standard and Technology Framework," *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 1, pp. 89–97, 2019, doi: 10.17781/P002567.

[30] W. Ahmed, F. Shahzad, A. R. Javed, F. Iqbal, and L. Ali, "WhatsApp Network Forensics: Discovering the IP Addresses of Suspects," *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France, Apr. 2021. doi: 10.1109/NTMS49979.2021.9432677.

[31] N. V. Vukadinović, K. C. Seigfried-Spellar, M. K. Rogers, U. Karabiyik, and E. T. Matson, "WhatsApp Forensics: Locating Artifacts in Web and Desktop Clients the Purdue University Graduate School Statement of Committee Approval," 2019, *Thesis*, University Graduate School Statement of Committee Approval, 2019, doi: 10.13140/RG.2.2.32589.28649

[32] S. Zakarneh and M. S. Scholar, "Forensic Investigation of WhatsApp on Android Smartphone's," *International Journal of Science, Engineering and Technology*, vol. 9, no. 4, pp. 1–7, 2021.

[33] G. Rotaru, "Mobile Forensic Tools: An Insight into WhatsApp Key DB Extractor," *Romanian Cyber Security Journal*, vol. 2021, no. 3, pp. 67–76, 2021.

[34] B. Ola, A. Arhin, and R. Asuming, "A Forensic Analysis of WhatsApp on Android smartphone," *International Research Journal of Computer Science (IRJCS)*, vol. 07, 2020, doi: 10.26562/ir.

[35] M. W. Indriyanto, D. Hariyadi, M. Habibi, U. J. Achmad, and Y. Yogyakarta, "Investigasi dan Analisis Forensik Digital Pada Percakapan Grup Whatsapp Menggunakan NIST SP 800-86 dan Support Vector Machine,", *CyberSecurity dan Forensik Digital*, vol. 3, no. 2, pp. 34–38, 2020, doi: 10.14421/csecurity.2020.3.2.2193

[36] S. H. Jayady and H. Antong," Theme Identification using Machine Learning Techniques," *Journal of Integrated and Advanced Engineering (JIAE)*, vol. 1, no. 2, pp. 123-134, 2021, doi: 10.51662/jiae.v1i2.24

[37] A. Mahajan, M. S. Dahiya, and H. P. Sanghvi, "Forensic Analysis of Instant Messenger Applications on Android Devices," *International Journal of Computer Applications*, vol. 68, no. 8, pp. 975–8887, 2013, doi: 10.5120/11602-6965