IJASST
International Journal of
Applied Sciences and Smart Technologies
p-ISSN 2655-8564, e-ISSN 2685-943, pp. 63-98, 2024

Volume 06
Issue 01

Mobile Forensic Investigation on iOS & Android Smartphones: Case Study Investigation on WhatsApp

Shadi K. A. Zakarneh[1*]

[1]*M.Sc. Student, Palestine Technical University- Kadoorei, Tulkarem, Palestine,*

zakarnehshadi@gmail.com

(Received 03-07-2023; Revised 01-04-2024; Accepted 25-04-2024)

Abstract:

Following the exponential growth of information and communication technologies, the smartphone market, as well as advances in wireless data networks (3G and 4G), has accelerated. Mobile apps for social networking and instant messaging have been created by these firms. Other instant messaging (IM) smartphone programs like WhatsApp (WA), Viber, and IMO have also been created. WA is the most widely used instant messaging program. With WA, you can send and receive messages in a variety of formats, including text, voice, video, and documents. Various cybercrime incidents were committed through WA's. WA use leaves several artifacts that may be examined to detect the digital evidence. In addition, iOS and Android are two of the most popular smartphone operating systems. Because of this, the inquiry will involve the use of forensic investigative techniques and methodologies. Forensics on both iOS and Android cellphones were utilized to investigate a digital crime that was believed to have been perpetrated in WA. To conclude the investigation, we analyzed chat logs, phone records, and other media to gather proof. Legal framework and established processes were used to guarantee that evidence was preserved from change or destruction and that the witness's account was acceptable in court throughout the investigative process. It was finally stated that the inquiry and evidence had been presented. As a result, WA forensic artifacts might be evaluated and found effectively utilizing the mobile forensic procedure.

Keywords: WhatsApp; Forensic; iOS; Smartphone; Seizure; Acquisition; Analysis; Investigation.

1 Introduction

Many virtual communication apps have emerged as a consequence of the quick and huge expansion of communications and the Internet, such as social networks and IM programs such as Facebook, Twitter, Snapchat, Skype, and WhatsApp (WA). These

This work is licensed under a Creative Commons Attribution 4.0 International License

innovations have made communication between individuals easier, faster, and free, as well as removed geographical barriers [1].

As a consequence of the advancement of technology and communication, cellphones have supplanted PCs in many applications because of their portability, affordability, and low energy consumption; this trend is expected to continue [2]. Also, Some fundamental mobile phone services, such as SMS, have been superseded by IM programs [2].

Among the many IM applications on smartphones, WA is the most widely used IM service [3]. According to a Statista report from October 2020, the most popular and widely used IM app based on the number of monthly active users would be WA [4], WA is the most used by 2 billion active users, followed by Facebook Messenger 1.3 billion, WeChat 1.206 billion, QQ 648 million, Snapchat 433 million, and the Telegram has 400 million active users, as shown in Fig. 1.

For illegal reasons, the widespread usage of WA, as well as the vast range of material that may be shared over it (text messages; photos; videos; audio files; etc.), makes it hard to prohibit WA from being used [2]. Several artifacts occur from WA calls and messages. A forensic examination is carried out on these artifacts to get evidential information [3]. Although cybercrime is on the rise and may be used for a wide range of bad intentions, it is more common to do it for personal gain, business gain, intellectual property theft, personal theft, bullying, harassment, and even terrorism. Law enforcement must be involved in the investigation and prosecution of cybercrimes at all times [5]. As well, cybercrime, its tools, categories, and criminals must be defined under particular legislation. As a result, specialist law enforcement entities must be established to investigate and deliver this information to the courts. In addition, it is necessary to update the criminal code to reflect this new category of offense [6].

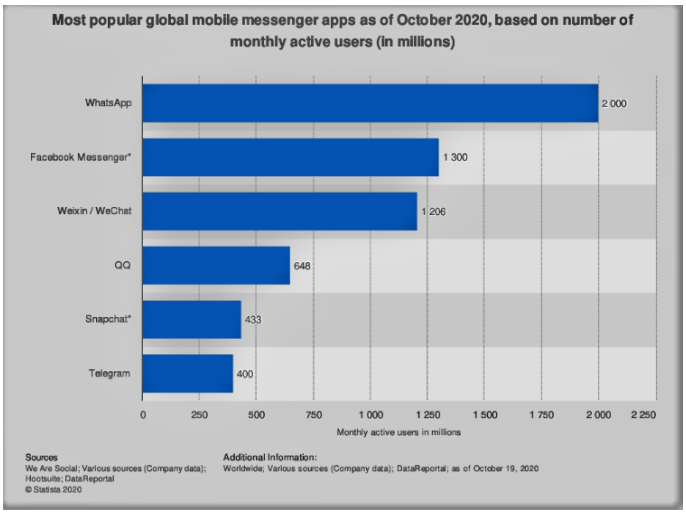


Figure. **1**. Mobile instant messaging applications statistic [4]

Most countries around the world are issuing cybercrime laws. Specialized law-enforcement agencies are also founded to investigate this type of crime [7]. The state of Palestine and many other countries issued a cybercrime law by Decree No. 10 of 2018. This law defines activities, tools, and terminology related to cybercrime, and determined the law enforcement agencies that are responsible for the investigation and prosecution of cybercrime and the penalties for these crimes [8].

This research aims to explore the artifacts in WA on iOS and android platforms and the use of tools related to the digital investigation to access digital evidence in WA by extracting messages and calls, analyzing them, and linking them in a chronological sequence to reach the digital evidence of the case.

2 Literature Review

WA is independent on smartphone platforms, as it works on different platforms such as iOS, Android, Windows Phone, and Symbian. In addition to that WA is a free charge application for most platforms, and it is charge-free in sending text, voice, images, and video messages [9].

2.1 iOS Operating System

The iOS operating system developed by Apple, iOS constitutes the primary platform for Apple mobile devices [10]. This system controls all services and parts of Apple

devices. the iOS operating system was launched for the first time in the year 2007 with the launch of the first iPhone device, where the name of the operating system was OS X, after that the name was changed in 2010 to iOS [11]. The iOS operating system architecture has four layers which are the core OS, core services, media, and Cocoa Touch layer [12].

The iOS operating system acts as an intermediary between the applications running on the screen and the hardware components of the device. iPhone has two partitions, the iOS system partition and the iOS data partition [13]. The contents of the iOS system partition maybe not be evidentiary which is used for the operating system and read-only for the user, but it may be necessary to examine it [13]. The iOS data partition is used as a read/write for the user and the applications so the evidence can be acquired from this partition [13]. iOS performs its roles through four layers [11], as shown in Fig. 2.

The top layer of the iOS architecture**,** This layer consists of a set of basic frameworks for developing the visual interface and providing the basic infrastructure for applications on the iOS system such as touch, multi-touch, input services and processes, and high-level tasks [11]. This application consists of basic multimedia frameworks such as audio, video, and graphics. This layer provides an aided environment for programmers to create

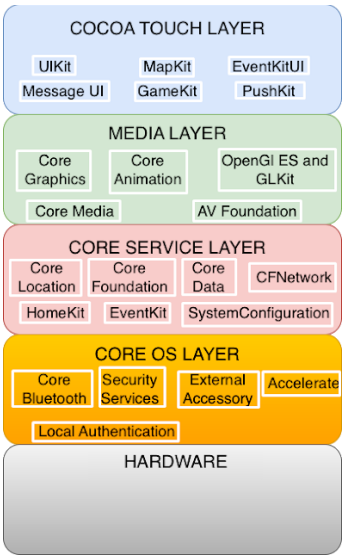


Figure. 2. iOS layered Architecture [14]

applications with a distinctive graphic appearance [11]. This layer works to provide the basic services required for applications on the system, such as location services, communication services, and iCloud services [14]. This layer is located directly above the device's hardware, and it deals with basic, low-level functions in the device, such as memory management, file system, communication, and networking [11].

2.2 Android Operating System

Android is an operating system for mobile devices developed by Android Inc., then Google bought it, and it was bought finally by the Open Handset Alliance. Android is based on the Linux kernel. Android Platform can be used on different hardware with different mobile phone manufacturers. Because android integrates seamlessly and robustly with Google products and strongly supports cloud computing, making it the best operating system for mobile devices [9].

Android OS is an open system architecture using a hierarchical structure. As shown in Fig. 3 android structure is divided into five layers [9]. Linux 2.6 kernel is the android OS base layer, as this layer is responsible for the basic functions of the system such as memory management, process management, device management, and power management. Linux kernel provides better interaction with the peripheral devices in the smartphone [16].

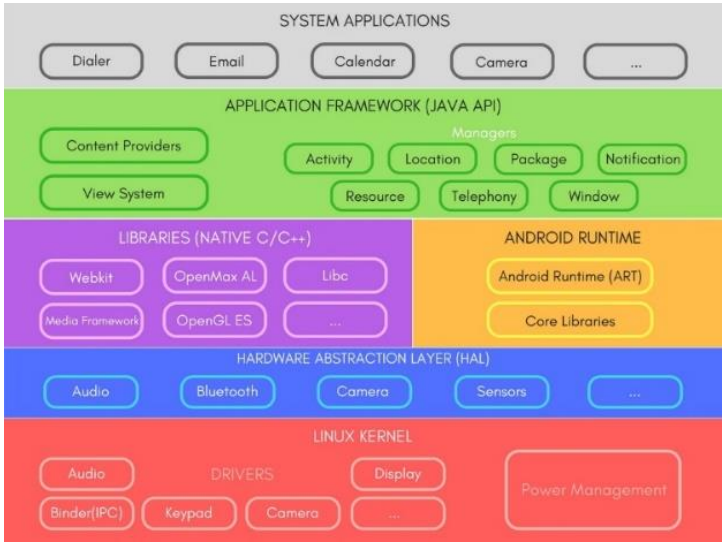


Figure. 3. Android Architecture [15]

The hardware Abstraction (HAL) layer is above the Linux kernel layer. This layer provides an interface between system services and device drivers for those services. It makes Android neutral concerning low-level drivers [17]. The Android system includes a set of main basic libraries that are exposed to developers through the Android application framework; these libraries are SQLite, FreeType, Webkit, OpenGL ES, and Media Framework. These libraries are written in C ++, and they enable the device to deal with different types of data [17].

The basic functions of the device are managed by the application layer. This layer provides user applications with application programming interfaces (APIs) that are used by applications for several purposes including getting notifications, accessing the telephony system, and sharing data. The application framework consists of an activity manager that works to manage application activity, content providers responsible for managing data sharing between applications, a location manager that works to manage locations through GPS, a telephony manager responsible for managing voice calls in applications, and managing the various resources used In applications by the resource manager [16].

The Applications layer is the top layer in android architecture, it includes the basic applications such as the contacts manager application, the SMS application, the dialer application, and the web browser application. This layer also includes applications that are developed by third parties. Since third-party developers have access to this layer, they can re-develop some basic features and applications such as the user interface and other applications to replace the basic applications of the system, this is a strong feature of the open-source Android system. Applications are written by developers in java. The developed applications are interpreted by the Dalvik virtual machine, which is replaced by Android Runtime (ART) [16].

Android OS uses a file system to organize the data on storage; the efficiency of the file system depends on the speed of storing, reading, and retrieving data. The file allocation system 32 (FAT32), yet another flash file system 2 (YAFFS2), and extended file system (EXT) file systems are used in the Android platform. These systems are used to operate the device, boot, store, and retrieve data. Also, These systems are used to organize data and files on SD memory. On flash memory, the YAFFS2 file system is used [17].

2.4 WhatsApp (WA)

WA is a popular IM application on smartphones. WA allows users to exchange text messages, images, video files, audio files, and many other types of files such as document files, pdf files, and others. WA allows users to create user groups to send messages and files to all group members. WA also allows the user to control personal profile information such as name, profile photo, and information about the user [18]. WA messaging is done in end-to-end encryption, and therefore no man-in-the-middle can read messages between two WA users [19]. WA stores its data in the mobile phone's internal memory. WA automatically connects to the phone contacts database, detects the contacts that use the WA application, and adds them to its database. WA application also includes a procedure named "com.whatsapp", which is a procedure for operating the external media management service and the messaging service that runs in the background, as this procedure works when turning on the smartphone [20]. WA used the SQLite database "ChatStorage.sqlit" to save messages that were exchanged between users and other information from the user activities on WA [10].

Old versions of WA used the SQLite database "msgstore.db" to save messages that were exchanged between users, this database was unencrypted. Because unencrypting the database, led to easy access to the details of the messages stored in it, to bypass this problem and achieve better protection for users' privacy, an encryption mechanism was developed for the WA database on the Android platform using Advanced Encryption Algorithm (AES) with an encryption key 192-bit length. As a result, the database name has changed to msgstore.db.crypt, msgstore.db.crypt5, msgstore.db.crypt7, and msgstore.db.crypt8. In recent versions of WA, the AES algorithm was used with a 256-bit key and the database became msgstore.db.crypt12 [20].

Research studies mostly deal with forensic methodologies on various mobile applications, such as forensic analysis of contact lists, SMS messages, and social media. Some researchers have compared several analysis tools by applying them to the analysis of processes for obtaining WA messages and files on android platforms. Other researchers determined different artifacts on android platforms generated by WA such as contacts database, messages database, and the database encryption key. (Shidek, Cahyani, and Wardana, 2020). Another study focused on the decryption of WA encrypted

databases, in this study, the researcher used five different tools to achieve his goals; these tools are WA key/db extractor, WA viewer, WA extract, SQLite spy, and android backup extractor. Some of these tools are written in python code, so a python compiler is also needed in their experiment [21]. A comparison study between two forensic tools for examining iPhone devices [13]. The study showed a comparison between Elcomsoft iOS Forensic Toolkit and Oxygen 2012 in terms of the ability of these tools to examine non-jailbreak and jailbreak iPhones [13]. This study focused on mobile forensic investigation in WA on iOS and Android platforms using a variety of digital forensic tools.

3 Research Method

This study's goal is to undertake a forensic assessment of Android and iOS cellphones. To perform the mobile forensic steps and evaluate the evidence gathered from WA, a hypothetical scenario will be utilized to simulate the case. This concludes the mobile forensics investigation report writing process.

The scenario illustrates the perpetrator using phone calls and text messages sent through WA to exert blackmail pressure on the victim. When dealing with evidence, the investigator has to follow the mobile forensic procedure to grab it, make sure it's safe, and keep it from being altered in any way. After that, the data from the evidence image is recovered so that investigators may investigate the discussions, phone calls, and photographs that took place between the perpetrator and the victim when they were communicating through WA. In this circumstance, the smartphone is in a capable position to be switched on since it is already operating.

Fig. 4 shows the mobile forensic method that was employed in the simulation. To deliver a witness report to the court, all necessary efforts were done to acquire legitimate and acceptable evidence.



Figure. 4. Mobile Forensic Process

For the seizing step, a legal body such as the Public Prosecution must issue a reasoned and specified search warrant. Defining digital evidence in a search warrant is essential. Digital evidence seizures are conducted by professional law enforcement officers or digital investigation specialists accompanied by court authorities to guarantee that digital evidence is safe and secure. This is also a time to make sure that all the protocols used in the seizure process are followed, as well as the laws governing personal privacy and individual rights. As part of their duties, judicial seizure officers are responsible for securing and documenting the crime scene. There are further documents that are included with a seizure report that include a list of confiscated devices and their owner's identity. Remaining in their original state is the goal of the preservation effort. Disconnecting the devices' wireless networks and any communication signals is also necessary to avoid any alteration or destruction of the digital evidence.

Forensic tools are then used to analyze and verify the evidence on the smartphone's backup and image data. The data imaging procedure was carried out with the help of the Final Mobile Forensic tool in this investigation. During the acquisition step, this procedure is carried out.

Data acquisition from a confiscated mobile phone was done using a logical acquisition, whereby the internal memory was backed up, the backup image was put in a storage medium to safeguard it, and the analysis procedure was performed afterward. Finally, the information gleaned from this procedure will be recorded and documented in a report. This information contains the name of the file, its size, and the MD5 hash value of the file, as well as the time and date of the image acquisition.

Using the previous stage's photograph, the investigator was able to do further investigation into the crime. Using the WA database, you may search for and view the evidence. The investigator checks the integrity of the evidence picture by recalculating the image hash value (MD5) and comparing it to a hash value obtained during the acquisition procedure.

A report will be issued when each step of the inquiry has been completed. There is information on the investigator and an introduction to the crime in this section of the file. Documentation of all evidence gathered, including a timeline of events, is

included in the report's findings. For the report to be acceptable in court, all operations must be conducted following the law and recognized procedures.

4 Experiment

Based on the Anti-Corruption Commission's legal competence to accept and examine allegations of corruption, based on the legislation enacted by decree No. 7 of 2010 to fight corruption. Seizure and investigation methods, in addition to the measures that have already been established. The following are the first steps taken in the envisioned scenario:

1- Following a claim by a victim of corruption, an investigative department issued a search warrant for a suspect based on anti-corruption and cybercrime laws, according to a statement from the Palestinian Anticorruption Commission.

2- A digital evidence seizure procedure based on Decree No. 10 of 2018 on cybercrime has been sought by the investigation department's judicial officials, who have asked for the aid of digital investigation specialists.

4.1. Seizure Stage

Based on an anticorruption prosecutor's search order granted under article 32 (paragraphs 1 and 2) of the legislation on cybercrime, this step was carried out. A seizure report based on Articles 32 and 33 was used to capture the following facts throughout the seizure process:

1. **The Reporting agency:** Anticorruption commission/ Digital Forensic Department.
2. **Case Identifier:**

   Investigative Case No: 20/2021. (Assumption)

   Digital Forensic Case No.: 7/2021. (Assumption)
3. **Forensic Investigator:**

   Job ID NO.: 00046.

   Name: Shadi K. Zakarneh.

   I am a computer systems engineer. I have experience in digital forensics and information security. I am a general director of the information technology directorate in the Palestinian Anti-corruption commission. I am now a master's degree student in

Science in Cybercrimes & Digital Evidence Analysis program at Palestine technical university – Kadoorie.

4. **Identity of the submitter:** Anticorruption commission/ Investigation Department.
5. **Date of the evidence receipt:** 20/04/2021.
6. **Details of the seized devices: are** shown in Tables 1 and 2.

Table 1. the iPhone Seized device details

Device category	Smartphone
The Owner	The mobile is owned individually by XXXXX
Make	Apple IPhone 11
Model No.	MWM42HB/A
Serial No.	F4GZW027N73H
IMEI	356562105937766
MEID	35656210593776
ICCID	899702812233269067083
iOS Version	14.4.2
Internal Storage	128 GB
External Storage	No
SIM carrier	Jawwal
Passcode	The mobile passcode is: 989429 “Provided by the suspect”
Front Color	Black
Back Color	Yellow
Power state	Power ON
Battery Charge Percentage	79%
Mobile external case	No Damages, No Scratches
Device Photographs	proposed

Table 2. The Android Seized device details

Device category	Smartphone
The Owner	The mobile is owned individually by YYYY
Make	Samsung
Model No.	Galaxy J6 SM-J600F
Serial No.	RF8KA38324A
IMEI	356423092355498
Android Version	Android 10 with Knox version 3.5
Internal Storage	32 GB
External Storage	No
SIM carrier	Jawwal
Passcode	12345 provided by the suspect
Front Color	Black
Back Color	Black
Power state	Power ON
Battery Charge Percentage	95%
Mobile external case	No Damages, No Scratches
Device Photographs	proposed

Suspected gadgets were turned on and remained on throughout the seizure procedure. In addition, airplane mode was selected on the devices. Wireless connectivity was cut off. To confirm that all radio signals have been removed, a Faraday bag is utilized. Deed 10 of 2018 on cybercrime mandated certain steps to safeguard digital evidence under article no. 33 (paragraph 5).

7. Tools used in the seizure process

The documentation of the process: handwriting documentation.

Photography: Digital Camera used.

To ensure signals are disconnected: a Faraday bag is used.

8. Chain of Custody documentation

Documentation of the confiscated device was completed at the same time. The owner's name, investigation case number, digital forensic case number, and receipt date are all printed on the device. Next, it's stored in a secure location until the next step in testing. The name of the digital forensic examiner is also included in the record of this information.

4.2. Acquisition Stage

Following Article 32 (paragraph 4) of the Decree No. 10 of 2018 on Cybercrime, the anti-corruption prosecutor issued a direct access warrant for this stage. The ADB backup command-line tools, the Belkadoft forensic tool, the mobiledit tool, and the final mobile forensic tool will all be utilized to collect data from the confiscated device. To connect the mobile device, we will utilize a Samsung small USB cable. Storage media will also be employed to store the obtained evidence picture. The purpose of the investigation and the facts necessary for the inquiry must be established before the investigation can begin.

The documentation information of this stage includes the following:

1- The examiner's name and information.
2- The suspect device details
3- The tools used in the process.
4- Date and time of the process.
5- The duration of the process.
6- The name of the image file.
7- Size of the image file.
8- The hash value of the generated image.

A warrant granted by the prosecutor's office allowed me to see it. As mandated by Article 32 (paragraph 4) in the Decree issued on December 10, 2018, the purchase was carried out. The logical acquisition was utilized when the device was unlocked.

4.2.1: iOS Acquisition

This step was carried out with the use of a variety of forensic instruments. Once iTunes was installed, more programs were employed to extract evidence from the device's backups.

For the Acquisition phase many software can be used to conduct this phase, The iTunes software is used to take a backup for the iPhone device. Also, Enigma Recovery Software can be used for iOS acquisition. In addition to DB Browser for SQLite that can be used to explore SQLite databases that are recovered from mobile devices. Moreover, the iBackup Viewer Pro tool can be used to explore iTunes local backup and explore and view the backup data.

One of the more popular mobile forensic software used is the Belkasoft Evidence Center, this software was used in the experiment to acquire the iOS evidence.

iOS acquisition using Belkasoft Evidence Center

Forensic investigators may access a smartphone's backup directly using this forensic tool, which allows them to do the logical or physical acquisition. An iTunes-created mobile picture was opened on the local computer and used to get this information.

1- Fig. 5 shows how the new case was produced in the Belksoft evidence center. Fig. 6 shows how the iTunes backup folder was loaded using a mobile image. Fig. 7 depicts the selection of relevant data and apps for the search. As may be seen in Figs. 8 and 9, the results of interpreting and obtaining the picture are rather impressive.

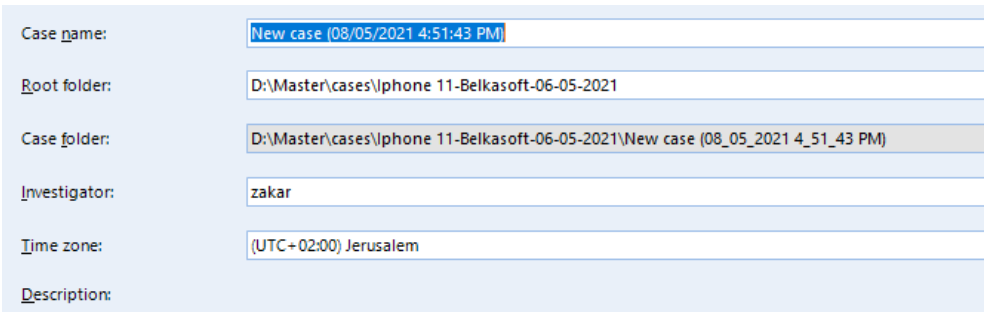


Figure. 5. Belkasoft Create a new case

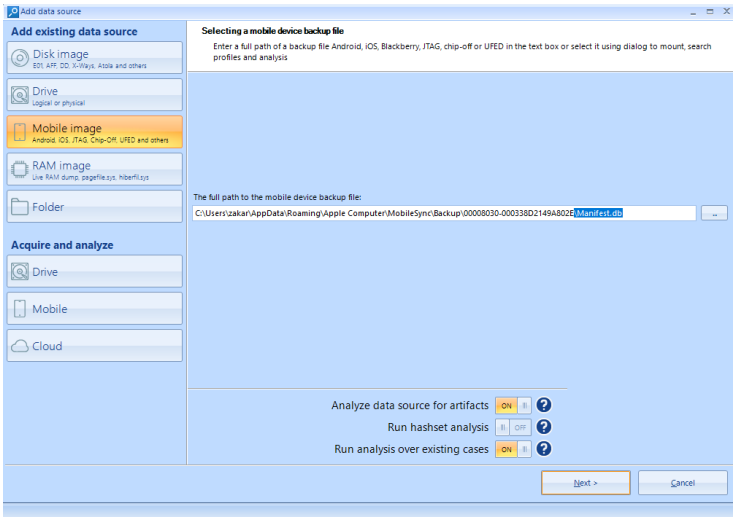


Figure. 6. Balkasoft determining data source

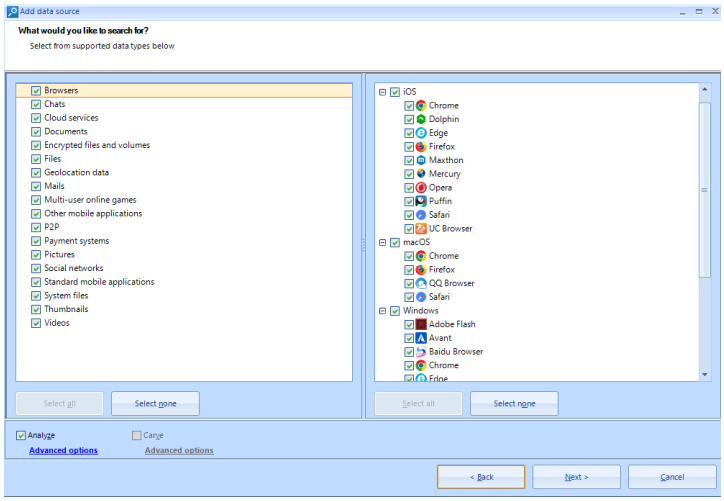


Figure. 7. Balkasoft determining what would you like to search.

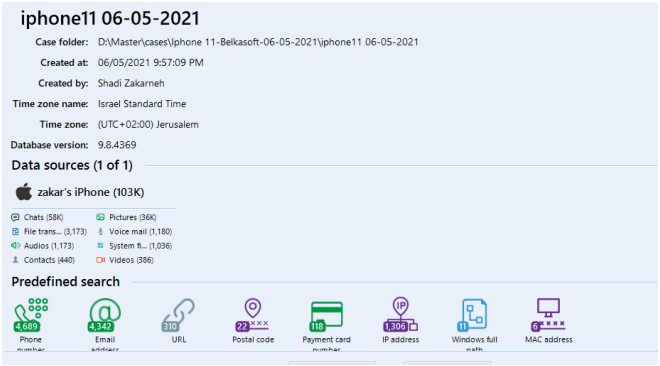


Figure. 8. Balkasoft backup reading and acquiring results



Figure. 9: Balkasoft: device information acquired from iTunes backup

4.2.2 Android Acquisition

Different tools can be used for android acquisition such as ADB command line tools, Before the logical acquisition, the developer options and USB debugging were enabled, Belkasoft evidence center forensic software, final mobile forensic software, and MOBILedit forensic software.

4.2.2.1 Android acquisition using ADB command-line tools

The result of the acquisition stage is documented as shown in Table 3:

Table 3. Documented information from the acquisition stage using ADB command-line tool

No.	Examiner Name	Shadi Zakarneh
1-	Suspect device details	As it is documented in the seizure stage and the acquisition tool record this information
2-	Acquisition tools	ADB command-line tools
3-	Date and time of the process	2021-07-07 14:19:09 ~ 2021-07-07 14:24:36
4-	Process duration	5 minutes and 27 seconds
5-	Acquired Folder name	J607072021
6-	Image file size	12.6 MB
7-	The hash value of the generated image	57B48282FC97403F827A0A173A0C12F2

ADB command-line tools were used to restore the mobile's backup before the purchase began. Open the backup files using the Belksoft evidence center and Final mobile forensics, and then extract the data. The purchase procedure will be described in depth in the following phases:

1- After identifying the suspect's device, the examiner compared the information to seizure information.
2- Fig. 10 shows the command-line tool ADB used to back up the device.
3- When the backup is finished, you'll get a backup of your data. An archived copy of an original file. Fig. 11 shows a tar file that may be utilized with forensic software tools.

4.2.2.2 Android acquisition using belkasoft evidence center forensic software

The result of the acquisition stage is documented as shown in Table 4.

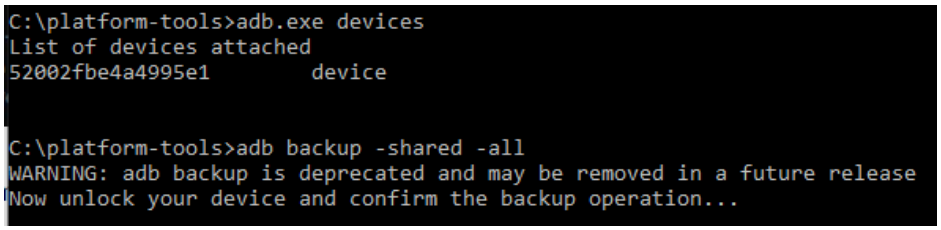


Figure. 10. ADB command lines to backup android devices

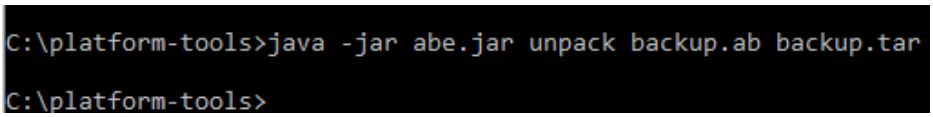


Figure. 11. Convert backup.ab file to backup.tar file

Table 4. Documented information from the acquisition stage using belkasoft evidence center

No.	Examiner Name	Shadi Zakarneh
1-	Suspect device details	As it is documented in the seizure stage and the acquisition tool record this information
2-	Acquisition tools	Belkasoft evidence center
3-	Date and time of the process	2021-07-07 18:11:17 ~ 2021-07-07 18:19:36
4-	Process duration	8 minutes and 19 seconds
5-	Acquired Folder name	Android\belka
6-	Image file size	14.9 MB
7-	The hash value of the generated image	AECCCE50E9338B1CD4167B522DB6E5B4

This procedure began with the creation of a case in the belkasoft evidence center and a backup of a mobile device. The purchase procedure will be described in depth in the following phases:

1- Fig. 12 shows how the data source was added to the constructed case by choosing the mobile data source and mobile type.
2- Belkasoft then established a connection with the device and displayed information such as the make, model, and type (see Fig. 13).
3- ADB backup creation began shown in Fig. 14.
4- According to Fig. 15, a backup operation was performed and the data written for analysis was picked.
5- Now the acquired data is ready for the analysis stage.



Figure. 12. Select data source in Belkasoft evidence center

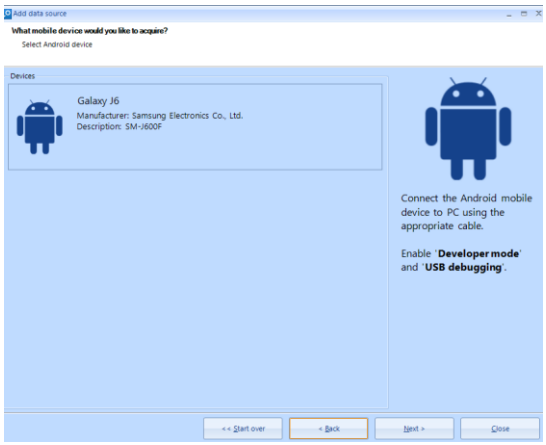


Figure. 13. Belkasoft evidence center connected with the device

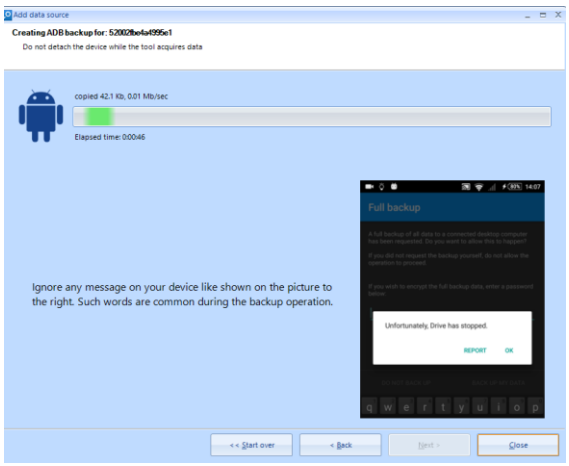


Figure. 14. Belkasoft creating ADB backup process

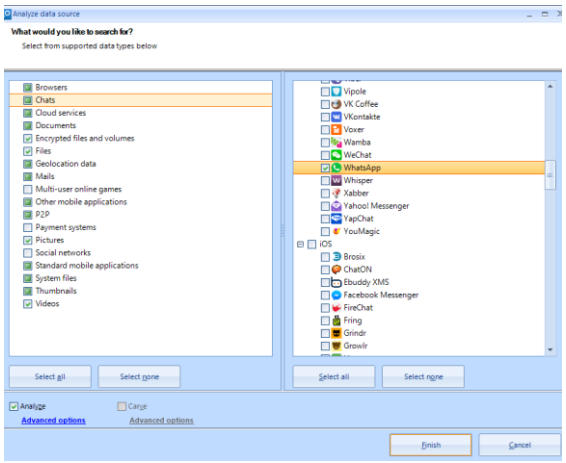


Figure. 15. Selecting the data types needed for the analysis stage

4.3. Analysis Stage

The analysis process succeeded as the evidence was found by reviewing WA chats and calls, as well as reviewing audio files, video files and photos exchanged through the WA application.

4.3.1 iOS Analysis

Using the iBackup viewer, the applications list in the manifest.plist files explored. By this tool, the WA version was determined and it was 2.21.72.1 as shown in Fig. 16.

iOS analysis using Magnet AXIOM Examine

Fig. 17 shows the dashboard information regarding the obtained case in Magnet Axiom Examine. The Magnet AXIOM Examine was able to categorize all items as illustrated in Fig. 18 by investigating them.

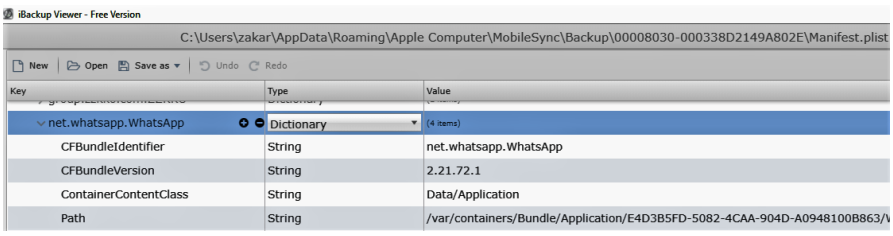


Figure. 16. WhatsApp Version from Manifest.plist file

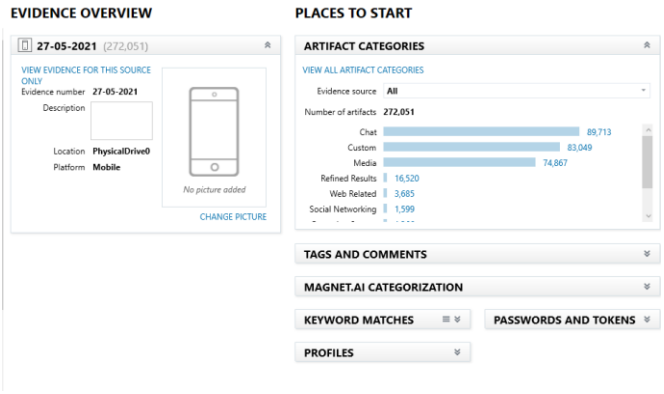


Figure. 17. Magnet AXIOM case dashboard

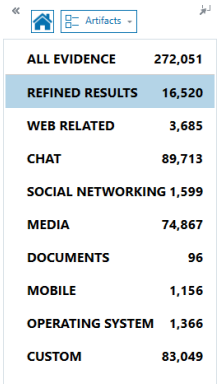


Figure. 18. Magnet AXIOM Examine Artifacts classification

While the focus of this research was on WA, the artifacts in the study may be used to evaluate the WhatsApp conversations, as demonstrated in Fig. 19. Magnet AXIOM Examine's artifacts module examines the logs of WA conversations, WA contacts, WA groups, and WA messages, as seen in Fig. 20. Fig. 20 depicts the WA chat logs available to the investigator, which indicate the names of individuals and groups, the chat ID, the most recent message sent or received, and the time and date of the most recent communication. Fig. 21 shows the account ID, phone number, complete name, given name, and whether or not the person is a current member of WA by examining the artifacts' WA contacts.

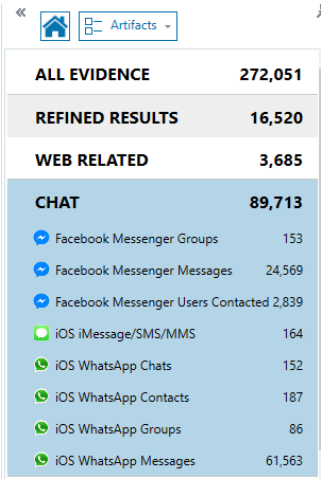


Figure. 19. WhatsApp Chats from the Artifacts view

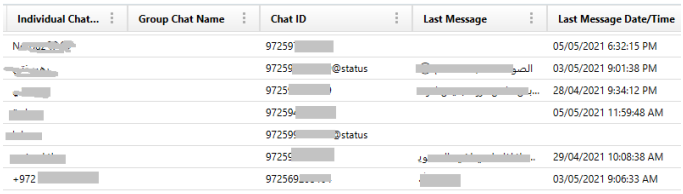


Figure. 20. WA chats log

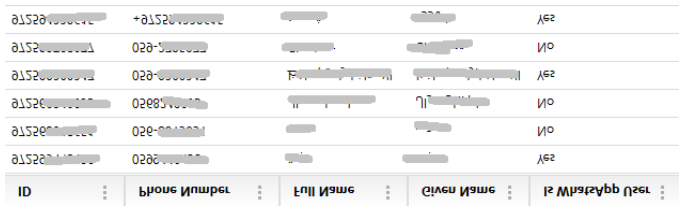


Figure. 21. WA contacts list

There is a lot of useful information about the user's participation in WA groups that can be gleaned from the artifacts, including the group chat id, the group name, the group's creator id, and the creator's name as illustrated in Fig. 22. As shown in Fig. 23, the WA messages from the artifacts may be used to examine a list of conversations, and by choosing any row of these logs as shown in figure 24, an investigator can access the chat information.

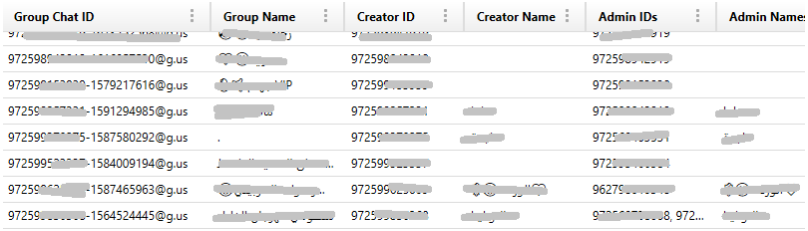


Figure. 22. WA chat groups

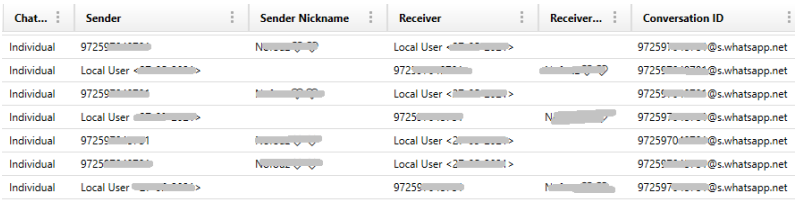


Figure. 23. WA chats list



Figure. 24. WA chats details in the preview pane

Fig. 25 depicts the discovery of WA SQLite databases while utilizing the file system for inquiry and browsing the WA folder. Belkasoft evidence center allows the user to search through the WA folder, as well as export the media files that are sent with friends by the user. However, with SQLite databases, a third-party program is required to access the data.

Artifacts module of Magnet AXIOM Examine was used to evaluate and read existing message lists on WA, as demonstrated in pictures 24 and 25. The interactions in WA were

also examined, as seen in figure 22. Figure 23 shows a list of the WA groups that may be seen in addition to the actual groups themselves. Images, files, and audio messages from the Message\media folder beneath the WA folder were also examined on a file system as part of the transferred media. When looking into the specifics of the chat conversations, it is possible to examine the accompanying media.

Android Analysis

Forensic tools such as Belkasoft evidence center, MOBILedit forensic, and Final mobile forensic tools were used throughout the analysis stage.

4.3.2.1 ADB command-tool backup analysis

Because the obtained device was unrooted, the ADB command-line tool's investigation of the backup file revealed that it included no files or data linked to WA. Figs. 26 and 27 in the Final Mobile Forensic and the backup file on the Belkasoft evidence center both helped to shed light on this.

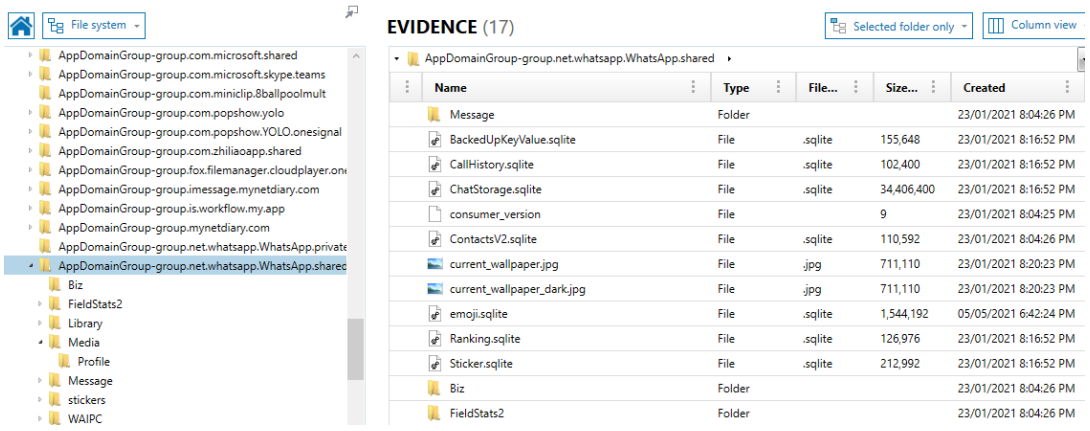


Figure. 25. WA folder in the file system

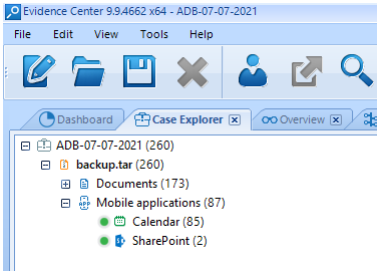


Figure. 26. ADB command line backup analysis using Belkasoft

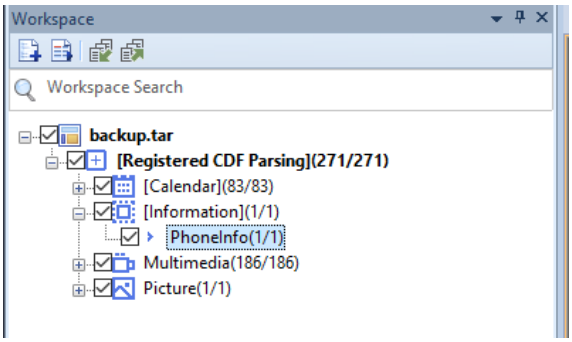


Figure. 27. ADB command-line backup analysis using Final Mobile forensic

4.3.2.4: Analysis using Final mobile forensic

The final mobile forensic was used to analyze the captured picture. Documentation and analysis of all of the digital evidence have been completed.

Fig. 28 shows how the WA account information appears in the final mobile forensic tool. Fig. 29 depicts the evaluation of WA's message lists, while Fig. 30 depicts the reading of existing message information and Fig. 31 depicts the viewing of deleted messages, texts, and attachments.

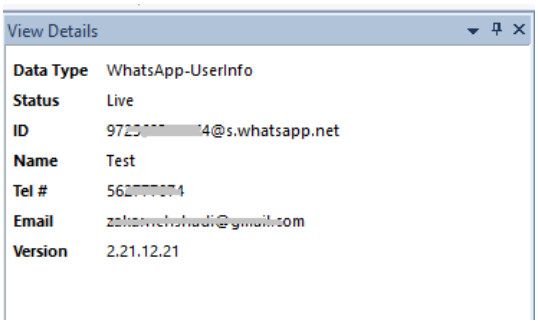


Figure. 28. WA account details in final mobile forensic

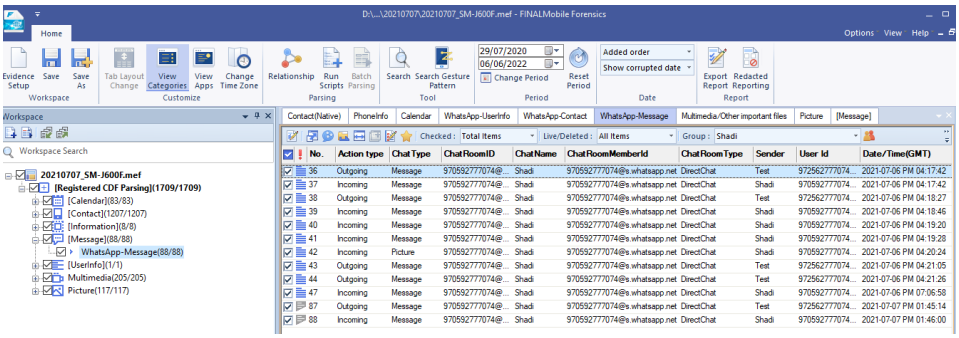


Figure. 29. List of WA messages using Final mobile forensic

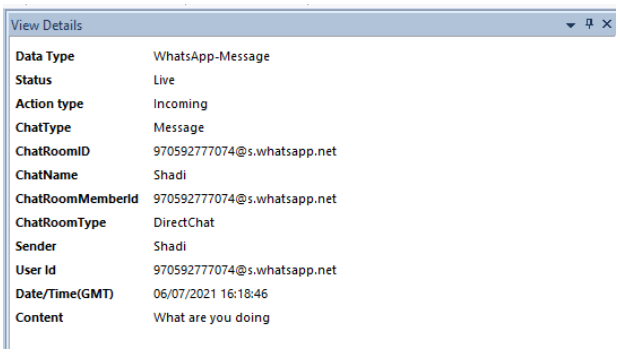


Figure. 30. Details of a live WA message in Final mobile forensic

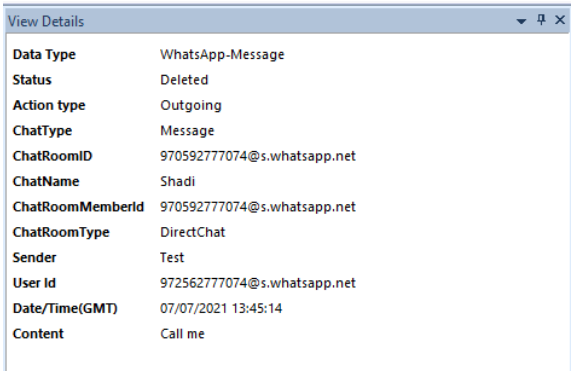


Figure. 31. Details of a deleted WA message in Final mobile forensic

Final mobile forensics may also be used to explore the file system to inspect and analyze the WA folder and its subfolders as shown in Fig. 32, and the WA SQLite database can be examined via an SQLite DB reader as shown in Fig. 33.

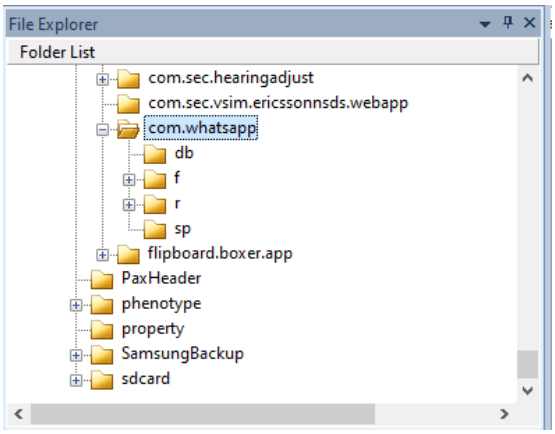


Figure. 32. WA folder and subfolders

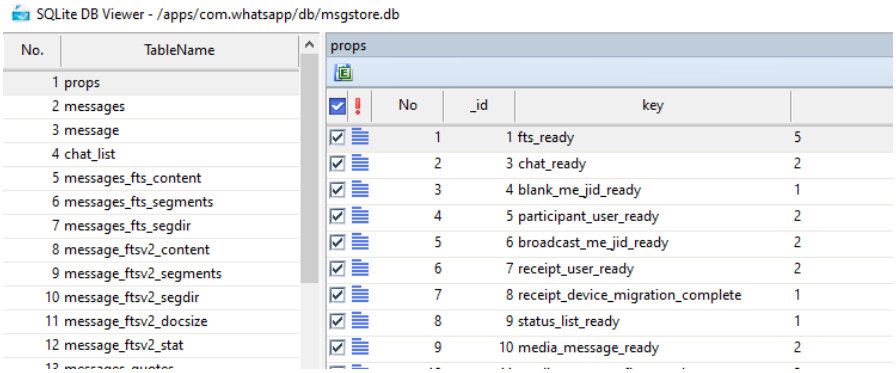


Figure. 33. WA SQLite DB

4.4 Android Mobile root

To get super user capabilities and complete access to the Android system, the root procedure was carried out.

In addition, the Samsung Galaxy J6 (SM-J600F), which was introduced in 2018 with an Exynos 7870 octa-core CPU and Android 10 with the Knox security feature, is among the devices being investigated. The root attempt was thwarted by the android version and security measures, despite the usage of a variety of tools and methods.

Rooting an Android smartphone requires the following:

1- Debugging through USB is enabled in the developer settings, as illustrated in Fig. 34.
2- Fig 35 shows how to activate OEM unlock to get access to the bootloader.
3- Fig. 36 shows how to put your device into download mode after a hard reset.
4- Boot image and custom ROM download.

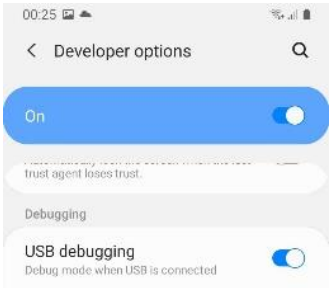


Figure. 34. Enable USB debugging on Android device

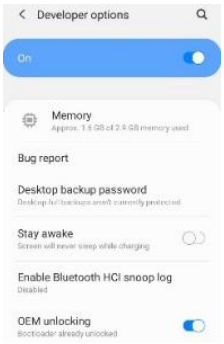


Figure. 35. Enable OEM unlock



Figure. 36. Android download mode.

Using the Odin rooting program, you can get root access to your Android smartphone:

1- Using a micro USB cable, connect the phone to the computer.
2- Open the Odin program, choose the custom image file, and begin flashing as shown in Fig. 37.

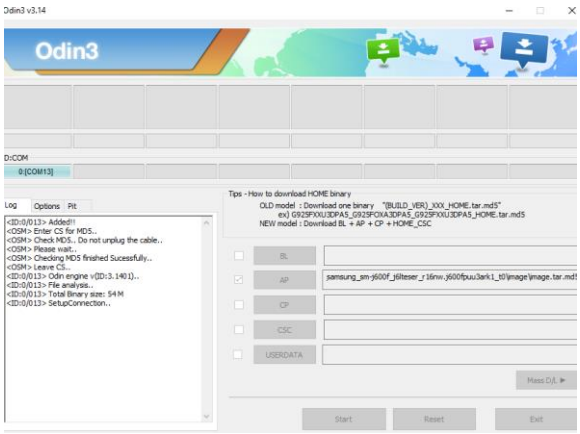


Figure. 37. Flashing custom image using Odin

Using the Magisk and Odin tools to root an Android device:

1- Magisk may be installed on an Android smartphone by following the steps outlined in Fig. 38.
2- Transfer the AP file from the custom ROM to the phone.
3- Use Magisk to apply the patch to the AP file.
4- Copy the patched file to the computer and add it to the Odin program, and then use Odin and download mode to flash the patched file to the mobile device.

Using the dr. fone-root program to root the android device as shown in Fig. 39:

1- Using a micro USB cable to connect the item to a computer.
2- Start the dr. fone-root process and the device will be detected.



Figure. 38. Magisk software for patching image.

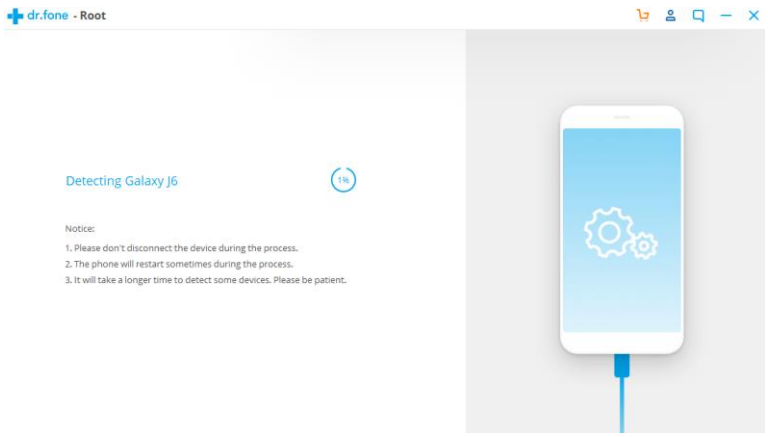


Figure. 39. dr.fone for rooting android devices

5 Results and Discussion

According to the approach, the investigation of WA messages was carried out on iOS and Android mobile devices using a variety of tools and methodologies.

5.1 Examination of the iOS platform

The investigation of WA communications necessitated the employment of a variety of techniques. iBackup viewer, Belkasoft evidence center, Magnet AXIOM analyze, Final mobile forensic, Enigma Recovery, and iBackup viewer were utilized for the inspection and analysis of the backup. In the acquisition phase, several of these tools don't allow for direct connection to the associated devices. Using iTunes backup or a logical backup is possible with one tool, but not with the other. The device's logical backup will not work until it first jailbreaks the device. A cybercrime conducted through the WA application was presumed for the purposes of this research; however, only files and data associated with WA were examined. There was no doubt that the examination process and the method in which the evidence from WA is viewed and presented varies significantly across all of these tools.

5.1.1 Examination of a backup taken by iTunes

The Belkasoft evidence center was used to evaluate and review the WA databases and files. SQLite viewer in Belkasoft may be used to examine and evaluate the database contents, which contain information such as contact information and group members. The databases' contents and structure are shown as tables in the SQLite viewer. In addition to the material that may be accessed from the chat's folder in the file system.

Using the Magnet AXIOM Analyze by looking through the WA folders, files, and database on your computer's hard drive. In addition, the artifacts' vital information for WA may be quickly accessed and categorized for a thorough analysis. Using a UI reminiscent of WA, the Magnet axiom was able to see the contents of the WA database as well as the chat messages. The data from WA required for the inquiry cannot be seen using a Final Mobile forensic. Enigma Recovery and the WA viewer allow you to see the data in the same way you see it in WA.

5.1.2 Examination of a backup taken from the connected iPhone device

Belkasoft evidence center, Magnet AXIOM analysis, Final Mobile Forensic tool, and Enigma Recovery are utilized to back up the linked device. Because the logical backup requires the device to be jailbroken to perform the logical backup, the backup option utilized is the iTunes Backup. When the device is backed up using the iTunes backup option, the results in the examination are the same as when the iTunes software backup is acquired from the local storage by the Belkasoft evidence center. iTunes backup failed on a high-storage device while running Magnet AXIOM on a forensic workstation because the program requires additional hardware. Only minimal data was saved from the linked devices, and this data was missing from the WA files and databases. It was possible to check the WA chat messages as they appear in other WA apps such as text or media messaging by using the Enigma Recovery program.

5.2 Examination of unrooted Android platform

For the investigation of WA communications, several technologies were utilized to collect and analyze data from a Samsung Galaxy J6 running Android 10 and the Knox security feature. ADB command-line tools were used for the acquisition stage, while Belkasoft evidence center and Final mobile forensic were used for the examination of the backup file that resulted. Forensic technologies including Belkasoft evidence center, MOBILedit, and Final mobile forensic were used in a second acquisition procedure.

5.2.1 Examination on a backup taken using ADB Command-line tool

Due to the unavailable storage location for WA on an unrooted device, the ADB command-line tool backup was not beneficial for the inquiry on WA.

5.2.2 Examination on a backup taken using Belkasoft evidence center

An ADB backup option with the ability to back up to shared storage was used to acquire the Android device. The Belkasoft evidence center was used to conduct an investigation, and the investigator discovered that there were no WA-related folders, files, or data.

5.2.3 Examination of a backup taken using MOBILedit forensic

As part of the purchase process, we used ADB logical backup. It was necessary to inspect the WA files and data when the capture was complete, thus the file system was

explored to do so. msgstore.db.crypt14 is the name of the encrypted WA SQLite database files. As a result, no SQLite DB viewer may be used to access the database. The WA folder's subfolders could be seen. Subfolders beneath the WA folder housed the images, videos, and documents that were delivered and received through WA (com.Whatsaspp).

5.2.4 Examination on a backup taken using Final Mobile Forensic

WA was degraded to an earlier, unencrypted version during the purchase process. To read messages and their information, the WA database was encrypted. Status (Removed) is applied to all messages that have been erased, but those that haven't been deleted appear as live. The SQLite database containing the messages may be exported and seen in the SQLite database viewer by browsing the file system and seeing the WA folder and its subfolders. It is also possible to examine and export all subfolders containing media files and documents delivered or received through WA.

5.3 Android mobile Root

It was unable to root the mobile device, even if the operating system was Android 10 with Knox security. Rooting an Android 10 device might be difficult since the ramdisk does not include the root file system. It is difficult to root the system since the root file system is integrated within the operating system. The Knox security feature also prevents any unauthorized image or custom ROM from being flashed or installed on the phone. Since the root cannot be found.

6 Conclusion

WA is the most widely used program for instant messaging, allowing users to share text messages, audio files, video files, and documents, as well as other types of multimedia. Forensic examination of WA on iOS and Android has been the subject of this study. The study uses the NIST digital forensic approach. Final mobile forensics, Belksoft evidence center, MOBILedit, and Magnet AXIOM are just a few of the technologies used throughout the inspection and analysis process. When it came to backing up the confiscated iPhone and the seized Android phone, ADB logical backup was employed. The texts, images, audio files, videos, and contacts of the alleged crimes are examined and studied during this phase of the investigation. An additional tool was

utilized to demonstrate the differences and capabilities of these tools in the examination process and the outcomes of extracting the digital evidence from WA on iOS and Android platforms. Using the NIST approach and the mobile forensic tools, an evidence from WA where collected and analysed including text messages, calls, images, so using these evidences the accused can be brought to court.

A future study may focus on rooting an android version 10 or above devices to extract more data in the acquisition phase. In addition to using different tools to acquire and analyse mobile devices to get more evidences.

References

[1] E. S. Han and A. goleman, daniel; boyatzis, Richard; Mckee, "Is whatsapp the future of workplace communication?: investigating the use of whatsapp in decision- making episodes," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2019.

[2] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile forensic tools evaluation for digital crime investigation," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, pp. 949–955, 2018, doi: 10.18517/ijaseit.8.3.3591.

[3] Ubaidillah *et al.*, "Analysis whatsapp forensic and visualization in android smartphone with support vector machine (SVM) Method," *J. Phys. Conf. Ser.*, vol. 1196, no. 1, 2019, doi: 10.1088/1742-6596/1196/1/012064.

[4] J. Clement, "Most popular global mobile messaging apps 2020," *Statista*, 2020. https://www.statista.com/statistics/307143/growth-of-whatsapp-usage-worldwide/ (accessed Apr. 20, 2021).

[5] I. Abdulai Sawaneh, "Examining the Effects and Challenges of Cybercrime and Cyber Security Within the Cyberspace of Sierra Leone," *Int. J. Intell. Inf. Syst.*, vol. 7, no. 3, p. 23, 2018, doi: 10.11648/j.ijiis.20180703.11.

[6] FBI's Internet Crime Complaint Center, "2019 Internet Crime Report," *2019 Internet Crime Rep.*, pp. 1–28, 2019, [Online]. Available:

https://pdf.ic3.gov/2019_IC3Report.pdf.

[7] A. Shahbazi, "Technological developments in cyberspace and commission of the crimes in international law and Iran," *J. Leg. Ethical Regul. Issues*, vol. 22, no. 4, pp. 1–12, 2019.

[8] PNA, "Law by Decree No. 10 of 2018 on Cybercrime," no. 10. pp. 1–15, 2018.

[9] S. AlHidaifi, "Mobile Forensics: Android Platforms and WhatsApp Extraction Tools," *Int. J. Comput. Appl.*, vol. 179, no. 47, pp. 25–29, 2018, doi: 10.5120/ijca2018917264.

[10] R. Gyorödi, D. Zmaranda, V. Georgian, and C. Gyorödi, "A Comparative Study between Applications Developed for Android and iOS," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 11, 2017, doi: 10.14569/ijacsa.2017.081123.

[11] F. Aleem, "Layered Architecture used by iOS and its Performance & Portability," 2019, no. July, pp. 0–19, doi: 10.13140/RG.2.2.22845.20968.

[12] C. Parth, J. Tamanna, and A. Animesh Kumar, "Comparative analysis of mobile forensic proprietary tools: an application in forensic investigation," *J. Forensic Sci. Res.*, vol. 6, no. 1, pp. 077–082, 2022, doi: 10.29328/journal.jfsr.1001039.

[13] D. Afonin, I. Hora, V. Kolesnyk, I. Popovych, and I. Kuchynska, "On the possibilities of using some modern three-dimensional modeling means in forensic examination," *J. Forensic Sci. Med.*, vol. 8, no. 1, pp. 17–23, 2022, doi: 10.4103/jfsm.jfsm_57_21.

[14] Rupesh, "iOS Layered Architecture," 2017. https://codeingwithios.blogspot.com/2017/09/ios-layered-architecture.html (accessed May 22, 2021).

[15] Studytonight, "Android Architecture - Software Stack of Android," *Studytonight Technologies Pvt. Ltd*, 2020. https://www.studytonight.com/android/android-architecture# (accessed Dec. 27, 2020).

[16] N. Ekanayake, "Android Operating System," no. July, pp. 1–11, 2018, doi:

10.13140/RG.2.2.20829.72169.

[17] J. Khan and S. Shahzad, "Android Architecture and Related Security Risks," *Asian J. Technol. Manag. Res.*, vol. 05, no. December 2015, pp. 2249–892, 2016.

[18] S. Udenze and B. Oshionebo, "Investigating 'WhatsApp' for Collaborative Learning among Undergraduates," *Etkileşim*, vol. 3, no. 5, pp. 24–50, 2020, doi: 10.32739/etkilesim.2020.5.92.

[19] H. Shidek, N. Cahyani, and A. A. Wardana, "WhatsApp Chat Visualizer: A Visualization of WhatsApp Messenger's Artifact Using the Timeline Method," *Int. J. Inf. Commun. Technol.*, vol. 6, no. 1, p. 1, 2020, doi: 10.21108/ijoict.2020.61.489.

[20] J. K. Alhassan, B. Abubakar, M. Olalere, M. Abdulhamid, and S. Ahmad, "Forensic Acquisition of Data from a Crypt 12 Encrypted Database of Whatsapp," *2 nd Int. Eng. Conf.*, no. October, 2017.

[21] G. L. Jhala KY, "WhatsApp Forensics: Decryption of Encrypted WhatsApp Databases on Non Rooted Android Devices," *J. Inf. Technol. Softw. Eng.*, vol. 05, no. 02, pp. 2–5, 2015, doi: 10.4172/2165-7866.1000147.

This page intentionally left blank