Forensic Analysis of WhatsApp

Authors:
Kevin Hjelmtveit

May 7, 2020

Forensic Analysis of WhatsApp

. *Executive summary-* **In this paper, we have dived deep into the messaging application WhatsApp. We looked into every aspect of WhatsApp and what makes it so popular. The paper starts with an introduction to the applications and how it is designed and its architecture also looking into the security aspect of it. Further, we discussed different techniques and tools for analyzing WhatsApp, we looked into how forensic analysis of different platforms (Android, iOS, Windows, and macOS) are performed and what information to expect, and where the information can be found within the platform. this paper has heavily looked into research papers to establish the standard of WhatsApp, including its security. Further, the paper has looked into the procedures of doing a forensic analysis of WhatsApp and what the outcome of these research has concluded.**

1 INTRODUCTION AND BACKGROUND

Recent technological developments have offered diverse solutions and strategies for overcoming the current challenges in communication, data sharing, and general interactions. When looking at communication technology, numerous solutions have been developed over the past years to overcome these challenges. WhatsApp is one of the revolutionary technologies offered today to foster communication and information sharing, there are other applications just like WhatsApp such as Facebook Messenger, Viber, Telegram, and signal to mention a few. All having the same goal of eliminating the barriers created through distance, delay, and privacy. But in a world with increased cyber risk, these applications have faced challenges to keep users information private and to gain the public's trust.

2 TECHNOLOGY

WhatsApp was developed in early 2009 [21] and did revolutionize communication and interactions within the modern community. WhatsApp has made communication and data sharing utilizing both mobile and web platforms easier. The lightweight application has been developed to offer solutions that meet the growing consumer needs from a communication dimension. The capacity to improve cross-platform communication has made it easy for the consumers to share information through various areas like the web, Android, and iOS. The initial idea behind this application and solution was to foster communication through textual and multimedia data. However, the technology has developed, accommodating numerous other advancements such as documents, videos, and other improvements. There are current developments to incorporate global payment solutions [17], which will improve speeds and transfer efficiency in sharing money across the globe. WhatsApp has grown to be one of the preferred smartphone applications in the recent past, regardless of the current issues concerning data privacy and security concerns. WhatsApp is an easy-to-use application where the users only need simple and basic information technology knowledge and skills to utilize it. Its ease of use has made it effective to adopt the underlying technologies to ensure maximum effectiveness.

With Facebook acquiring in 2014 [21] WhatsApp remains one of the most preferred applications utilized in various mobile and computing environments to foster communication. With the growing demands in communication, it has been easy for users to utilize WhatsApp to ensure data and

resource sharing efficiency. WhatsApp is currently used by an estimated 2 billion people globally [18]. With users demanding focus on privacy and security, applications such as WhatsApp have been involved with scrutiny of data leakage such as private information [2, 7]. The security of these applications is the number one concern among its users, so many users are willing to leave for other rivals [3].This became a reality on January 2021, WhatsApp announced changes to its privacy policy, making data sharing with Facebook mandatory for its users. If users don't agree to the new terms, they won't be able to read or send messages on WhatsApp. This was the last straw for many user, leading to people leaving the application for its rivals.

2.1 Landscape

WhatsApp is a lightweight application build from the Ejabberd server and uses the Extensible Messaging and Presence Protoco (XMPP) in communications management [22]. The XMPP, which is an open communication protocol designed for instant messaging is based on XML and allows the exchange of structured data between any two or more network entities [19]. This server has been used to foster messaging sent from one person to the other. Using the server, it is easy for users to share information and maintain reliable communication frameworks. On the same note, the application uses an agile approach in development and coding, making it easy to accommodate arising changes and updates. This approach has made it easy for the developers to continually monitor the application‘s health and progress, depending on the current trends in user interactions. The protocol adopted has facilitated data sharing and messaging across various platforms. This protocol is connected to the HTTP server, which makes it easy to integrate the web platform. Further, the application‘s performance is influenced by the FreeBSD operating system.

The application relies on the XMPP protocol and Mnesia database architecture to form the ultimate application infrastructure [22], WhatsApp also utilizes databases such as Postgress, MySQL, and Riak. These concepts and resources make it easy for developers to use the right interventions to come up with a reliable application. The YAWS (Yet another webserver) is where WhatsApp stores multimedia files. This application is based on the ContusFly model [11], which is one of the most common approaches and frameworks meant for designing and implementing smartphone systems. The applications architecture and framework are shown in figure 1.

The Communication that takes place on whatsApp are using Voice over IP protocol (VoIP) which allows communication regardless of location while utilizing only internet provider charges or WiFi connection. WhatsApp does utilize the signal protocol which is designed by open whisper systems [4]. This end-to-end encryption protocol is designed to prevent third parties and WhatsApp from having plaintext access to messages or calls. This was an issue up until version 2.8, messages were sent in plaintext [22].

WhatsApp have faced number of flaws since it was founded in 2009, In the table below we see some of the flaws related to security [20]:

- Januray 6 2012: Status change of an user was made possible as long as the phone number was known.
- August 2012: WhatsApp announced messages were encrypted to the latest version iOS and Android (but not BlackBerry, Windows Phone, and Symbian).
- March 2014: Someone discovers a vulnerability in WhatsApp encryption on the Android application that allows another app to access and read all of a user's chat conversations within it.

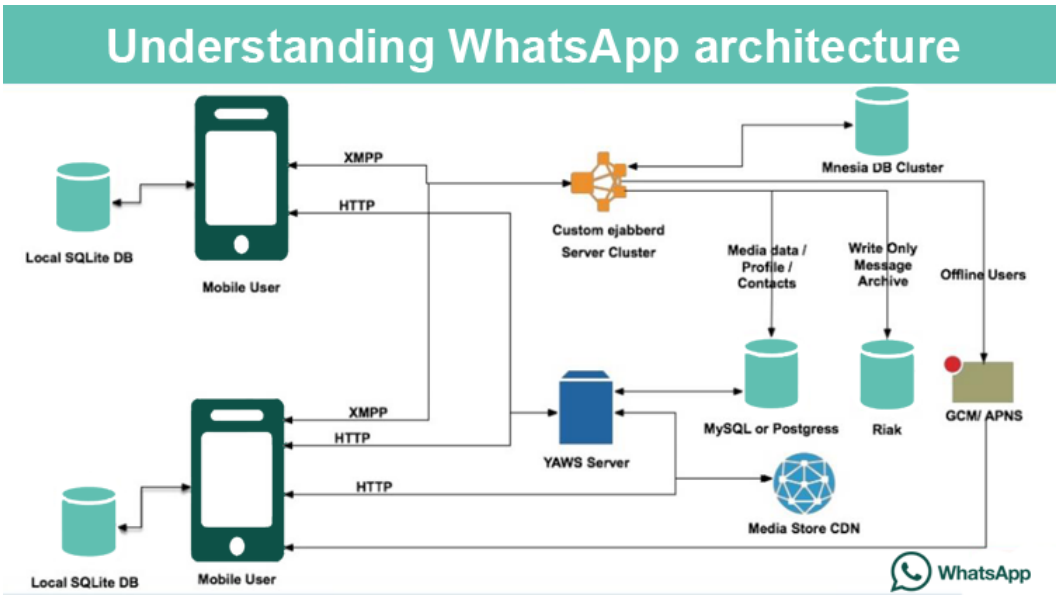

Fig. 1. WhatsApp architecture and Infrastructure [22].

- April 2016: WhatsApp and Open Whisper Systems announce that they finish adding end-to-end encryption to "every form of communication" on WhatsApp, and that users could now verify each other's keys.

WhatsApp is a great application and has a big user audience, but it is not perfect. some of the application's strengths and weaknesses need to point out, here few of them.

WhatsApp offers end-to-end encryption, it encrypts personal messages and business messages making it unreadable for others even WhatsApp. Like most applications, WhatsApp offers 2-step verification's making login more secure as it confirms that the user trying to see the application is the right user. WhatsApp offers both voice and video messaging, voice messaging utilizes your actual phone number, this has been a concern for some users. The application's availability is something to point out, WhatsApp is available on all platforms including on the web [16].

Every applications has it's flaws some of the biggest flaws of WhatsApp are it privacy, If anyone knows your number, they can see your profile pictures and the way you look without your consent. Another disadvantage is having random people you don't know add your number to groups without asking your permission. When sharing files on WhatsApp the maximum size of the file is 100 MB Another flaw on WhatsApp, is that there is no content censorship making users send inappropriate information across the network and combine this with the ability to add known numbers to groups without the users consent [16].

Earlier we mentioned how WhatsApp had announced changes to its privacy policy and how users were going to its rivals. As it stands now there are two prominent rivals Signal and Telegram. Of these two Signal provides better security, it utilizes end-to-end encryption by default on all messaging. Telegram only allows end-to-end encrypts one-on-one "secret chats", and this is something the user has to manually set. Signal only requires one thing from users and that is a phone number and

there is no attempt to link that phone number to your identity. Metadata is not collect by Signal like WhatsApp and Facebook Messenger do. Group conversations are also end-to-end encrypted with Signal, which is something Telegram does not offer [5].

3 ANALYSIS AND TOOLS

When considering the forensic analysis of a given application, the main goal is to gather evidence to use in supporting a given case or investigation. Numerous approaches have been used for forensic investigations and analysis associated with a given application. The effectiveness of the adopted measures and approaches may depend on the ability to define the channels and potential issues surrounding a given communication transaction [14]. WhatsApp forensic analysis involves using various tools and resources which facilitate data collection from multiple dimensions such as database and others. Further steps involves determining the kind of data being searched and identifying a reliable tool and technique to accomplish this goal. After determining the best tool, the other step is to collect evidence from the underlying smartphone making it easy to discover evidence to use in the court of law.

As a multiplatform application such as WhatsApp, makes use of forensics analysis and tools possible for different platforms, data acquisition can be acquired in multiple ways. If the device is available for the investigators, physical acquisition of the device itself is a good place to start. This includes the memory contains personal information management (PIM), contacts, calendar, SMS, voice messages, audio, and video calls logs etc [13]. Tools such as JTAG, FTK and Chip-off are used for hardware and image acquisition [12].
Logical acquisition works by acquiring a bit-by-bit copy of the storage logically. The biggest drawback faced is the ability to no recover deleted data. Otherwise, the logical acquisition is easy to perform. ADB pull, Backup analysis(SD card) and AFLogical are tools used for Logical acquisition[12].
To perform a software-based acquisition on WhatsApp root privileges are a must. Tools found for performing software acquisition are UFED, Oxygen Forensic suite, and another tool named "Whatsapp Xtract 2.0 -Zena Forensics" made by Francesco Picasso [9] which was able to encrypt and decrypt and SQLite database files to HTML format. The tool was useful for comparing data for analysis, faced problems since the tool was only able to present static information that was present in the database, when the data was deleted from the database no value was displayed.

Tools used for forensic analysis keep increase over the years, a study done by Radhika Padmanabhan et al. [10] where they took popular forensics tools such as SIFT, TSK Autopsy, Cellebrite, etc and compared the commercial versus the open-source forensics tools. The goal of the study was to find a "one-size-fits-all" forensic approach, the study had a broad list of criteria's which the tools were measured. The researchers concluded with there is no "one-size-fits-all", but some tools did perform better than others based on the criteria given. The result of the study can be seen in appendix figure 10. To use the software for analysis is straightforward, you simply download the tools and connect the phone to the computer, the software will then loop through your phone file system and find pre-defined file extensions or names within a specific file location.

3.1 WhatsApp artifacts on Android devices

When investigating and gaining artifacts on Android devices there a few steps that need to be taken. In order to extract artifacts from an Android device, the investigator needs to have root privileges. This can be done by either root the device or use software that that can extract a physical memory

dump of the file system [8].

Most of the application files are stored where the user's data is stored and can be found within the Userdata directory. This directory contains several subdirectories. Within these directories, there are many files where artifacts can be found. The most important files are two database files, the wa.db and msgstore.db. These are the main files for extracting artifacts on Android The wa.db contains important data such as lists of user's contacts, including phone numbers, display names, timestamps, etc. It also contains a table called wa_contacs where more detailed information about the contacts is stored.

The msgstore.db database contains information about the messages that have been sent, and information such as contact number, message content, status, timestamps, and information about attached files. The msgstore.db file is located under the path /data/data/com.WhatsApp/databases/. But maybe the most interesting table for a forensic analyst is the sqlite_sequence table, this holds information about the total number of chats, the total number of stored messages it also contains a file message_fts_content where the content of messages is saved.

3.2 WhatsApp artifacts in iOS devices

To gather artifacts on iOS there is a slight difference from Android. On iOS, the WhatsApp data is actually transferred to iTunes as a backup copy. This makes it possible to extract artifacts without the need for a file system, there is also a difference in the naming convention of the files and their locations. Like on Android there are files that are more important than others, on iOS most of the relevant data is stored in the ChatStorage.sqlite database and within the database, the interesting tables are ZWAMESSAGE and ZWAMEDIAITEM. ZWAMESSAGE, which contains the text contents of exchanged messages except for the media file. ZWAMEDIAITEM: All the media file sent is being indexed to correspond with data in ZWAMESSAGE.
Other tables important tables to look for are [8]:

- ZWAPROFILEPUSHNAME: Here the Whatsapp ID is being associated contact name
- ZWAPROFILEPICTUREITEM: Associates WhatsApp ID with a contact's avatar
- Z_PRIMARYKEY: Contains general information about the database, such as the total number of stored messages, the total number of chats, etc.

3.3 WhatsApp artifacts in Windows

When extracting artifacts in Windows, there are several places where they can be found. The Most important, directories that contain executable and auxiliary files. Which can be found in numbers places[8]:

- \Program Files (x86)\WhatsApp\
- \Users\%User profile%\AppData\Local\WhatsApp\
- \Users%User profile%\AppData\Local\VirtualStore\Program Files (x86)\WhatsApp\

The Local\WhatsApp\directory stores the file SquirrelSetup.log this file contains information and checks for updates and program installation.

The Users\%User profile%\AppData\RoamingWhatsApp\
On Windows the file main-process.log contains information about WhatsApp's operation. In Windows we also see a Databases.db file, but a difference from Android is that chat cannot be found in computer memory, but other multimedia files such as, documents and contact information was found.

, ,

3.4 WhatsApp artifacts in MacOS

WhatsApp artifacts in MacOS are very similar to what is found on Windows except for the naming convention of files and their locations. Places to look for an artifact on iOS are [1]:

- \Applications \WhatsApp.app
- \Applications\._WhatsApp.app
- \Users%User profile%\Library\Preferences
- \Users%User profile%\Library\Logs\WhatsApp

4 FORENSICS ON WHATSAPP

There have been several studies and real-world controversy about data leakage, data collection, and serious security risks concerning WhatsApp. This section highlights some of the studies and findings.

4.1 Scenario: WhatsApp Network Forensics

This research presented by Chang et al. [15], and looks at dissecting the communication payloads involved in a WhatsApp transaction between. This transaction involves multiple aspects, including servers from both the client and server sides and the respective communication payloads. This report aims to collect data about cybercriminal activity focusing on network forensics and relevant sniffing technologies. Their research can be segmented into four stages:

The first stage, which is data collection, offers a chance for collecting information such as the WhatsApp calling packets using tools like Wireshark. This packet sniffing tool has been successful in gathering information about various cyberspaces aiding the investigation processes.

The second step, which is data preparation, involved the researcher importing the captured packet information to Wireshark for further investigation. The second step involves using the Wireshark framework in analyzing the STUN protocol, which usually handles WhatsApp calling functionality. This step also involved preparing the captured data through exporting the pcap files to excel for further analysis. In the third stage, pattern recognition, the main focus has been determining similarities in the packets captured initially related to the suspects' and victims' IP addresses.

The last stage is data analysis, where the research team evaluated the collected data related to the investigation for further decisions. This research found that it is possible to evaluate the potentially criminal activities executed using the WhatsApp calling functionality. The research documented details such as the victim and suspect IP addresses address based on the inbuilt geo-location features and call-related details such as time and duration

4.2 Scenario: WhatsApp call signaling messages

This research presented by Baggili & Breitinger and speaks about WhatsApp network forensics [6] The research is explicitly addressing the decryption and analyzing the WhatsApp call signaling framework used in communication. This study was focused on gathering the initial WhatsApp calling feature forensic data, which can be used to inform decisions concerning data privacy and reliability. While WhatsApp has invested in encryption, the report using the right tools decrypted a sample calling signal intercepted from a smartphone to expose information like contact number, audio codec, call duration, and the server IPs.

The research process involved using numerous tools and approaches to support the experiment. Using an experimental approach allowed the research to document findings of the security of the WhatsApp calling feature. The experiment used a Python based command-line interface program named convertPDML.py. The experiment also used Wireshark as the initial data collection tool for capturing network traffic for further analysis. The first step was to disconnect the Android phone from the internet using password extractor to gain access to WhatsApp. The second step was to desynchronize the messenger from its web and client servers using pidgin. The third step was to set up a Wi-Fi access point to share the internet between the phone and the laptop used. After connecting the cell phone, the research made a WhatsApp call and captured the traffic using Wireshark. The next step was to analyze the captured traffic and decrypt it using the Wireshark dissector engine.

This report found out that it is possible to gain access to WhatsApp using various tools, most of which are available freely in the public domain. Using the Wireshark dissector engine, it is possible to decrypt a section of the captured traffic for further analysis. Further, after making the call and capturing the traffic, the research team decrypted it to gain access to essential details like WhatsApp password, phone numbers, phone call establishment, duration, termination, source, and destination IP addresses, and server relay.

4.3 Scenario: Whatsapp Contacts and Messenger exchange

This research is done by Anglano et al. [1, 8] the purpose of the research was to conduct what artifacts was left by Whatsapp Messenger on Android smartphones, Igor Mikhailov, a digital forensic analyst have also researched this topic with great results [8]. Anglano et. al was able to provide a list of database, log and various artifact files. Figure 2 in the appendix shows two of the most important files for Whatsapp forensics within Android. The wa.db stores information such as phone numbers, timestamps and display names as seen in figure 3 while msgstore.db store contact information about sent/recived text. Within the wa.db there is a table named wa_contacts which stores detailes information about the contacts seen in appendix A figure 4.

The researcher looked into the msgstore.db database and found interesting tables which contained useful information for forensic analysis. The most interesting tables within the msgstore database are message_fts_content and messages. The message_fts_content table actually contains the content of messages seen in figure 5 [8]. Within the messages table, we find more detailed information about the contacts seen in the figure 6.

4.4 Scenario: Reconstruction Contacts and contents of a message

Anglano et al. [1] were able to reconstruct a chat history by utilizing the databases and tables mentioned. The messages exchanged by the user which are stored in the message table need to be extracted and decoded for this to work.

In this example figure 7 show the contact number as 39348xxx, this is the contact number who we are contacting. the id is stored as key_remote_id.)From the tables received_timestamp and data, we can see that when this conversation took place, what the content of the message is. Here the key_from_me can either be zero(0) or one (1), the 0 representing false, meaning the message is coming from another person or device, while the 1 represents true and is the owner of the device.

Further in the figure, there is a reply from the owner (key_from_me='1') with the message "Reply 1". It's important to notice the key_id this key is unique and represents the two parties in the conversation. The researchers were also able to extract messages from delete contacts, this process was done by reconstructing a list of contacts that have been added in past and then comparing the

list with the current wa_contacts table and the contacts in the list that are found in the database have been deleted [1]. The research dived into how to extracting multimedia file an interesting aspect of the research is how to extract information from the media file. The first thing that happens when a file is sent, is that the file is copied into a folder named, then the file is uploaded to the WhatsApp server. When at the server, an URL is being sent back to the sender.

The sender then sends to the recipient a message containing this URL, when the message is received by the recipient, the recipient sends an acknowledgment back to the sender. The sender's message looks something like figure 8 as mentioned the media_url field stores the URL on the WhatsApp server temporarily. When transmitted the files are stored in the media_hash field encoded using base64 SHA-256 hash.

On the recipient side, most of the fields are identical seen in figure 9 . One thing to notice is the contents of media_url which is different except for the name of the file given by the server. The media name fill is set to null which WhatsApp detects as an unknown. This file can be identified by comparing the SHA-256 hash, by comparing the records that correspond with the files that have been received [1].

With this information, the file that has been sent by the sender and the one received by the recipient have similarities and can be correlated by comparing the file names given by the server and the SHA-256 hash values [1].

5 SUMMARY

There is no doubt that WhatsApp is a popular application, with its easy access and well-designed applications. The applications is performing well on all platforms (iOS, Android, macOS, and Windows) and the user satisfaction is high. Well as with every application, it has had problems in the past concerning security and performance. But has had a great improvement over the years, the application is robust and its security has improved. The architecture of the application is impressive and interesting to see how it evolved and how and integrated with Facebook. The forensics tools and analysis presented in the paper have been on various platforms, but mainly on Android. Android seems to be most of the user base and more research has gone exploring Android. This could simply be because of the Androids user-friendly configuration of the system, fewer permissions and restrictions comparing to iOS. The results from the different platforms were not too surprising, and had very similar outcomes. The different real-life scenarios presented are very interesting and show different ways to take advantage of the applications, but also show how WhatsApp's infrastructure on where the file are stored.

REFERENCES

[1] Cosimo Anglano. 2014. Forensic analysis of WhatsApp Messenger on Android smartphones. *Digital Investigation* 11, 3 (2014), 201–213.

[2] archyde. 2020. *Data leak in WhatsApp how to know if your phone number has been published in Google.* Retrieved May 20, 2021 from https://www.archyde.com/data-leak-in-whatsapp-how-to-know-if-your-phone-number-has-been-published-in-google/

[3] Kenny Chee and Cara Wong. 2021. *WhatsApp fights back over privacy concerns as users jump to Telegram and Signal.* Retrieved May 20, 2021 from https://www.straitstimes.com/tech/whatsapp-stresses-privacy-as-users-flock-to-rivals

[4] Whatsapp inc. 2020. WhatsApp Encryption Overview Technical white paper. https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-3&_nc_sid=2fbf2a&_nc_ohc=40tRbzve0awAX8PDm9q&_nc_ht=scontent.whatsapp.net&oh=1520d3a762062ee065721c8d0a84dc35&oe=6091B399

[5] john Bogna. 2021. Is WhatsApp End-to-End Encrypted, and Does That Matter for Privacy? https://www.howtogeek.com/722911/is-whatsapp-end-to-end-encrypted-and-does-that-matter-for-privacy/

[6] Filip Karpisek, Ibrahim Baggili, and Frank Breitinger. 2015. WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages. *Digital Investigation* 15 (2015), 110–118.

[7] Edex Live. 2021. *In a major data breach, numbers of WhatsApp web users found on Google search.* Retrieved May 20, 2021 from https://www.edexlive.com/news/2021/jan/15/in-a-major-data-breach-numbers-of-whatsapp-web-users-found-on-google-search-17312.html

[8] Igor Mikhailov. 2019. WhatsApp in Plain Sight: Where and How You Can Collect Forensic Artifacts. https://www.group-ib.com/blog/whatsapp_forensic_artifacts

[9] S Thakur Neha. 2013. Forensic Analysis of WhatsApp on Android Smartphones. *New Orleans– 2013-http://josemilagre. com. br/blog/wp-content/uploads/2014/03/Forensic-Analysis-of-WhatsApp-on-Android-Smartphones. pdf* (2013).

[10] Radhika Padmanabhan, Karen Lobo, Mrunali Ghelani, Dhanika Sujan, and Mahesh Shirole. 2016. Comparative analysis of commercial and open source mobile device forensic tools. In *2016 Ninth International Conference on Contemporary Computing (IC3)*. IEEE, 1–6.

[11] Ramanathan. 2021. Build a WhatsApp like Chat app in Android iOS Know How WhatsApp Works Technically. https://blog.contus.com/how-whatsapp-works-technically-and-how-to-build-an-app-similar-to-it/

[12] Sneha C Sathe and Nilima M Dongre. 2018. Data acquisition techniques in mobile forensics. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)*. IEEE, 280–286.

[13] Taniza Binti Tajuddin and Azizah Abd Manaf. 2015. Forensic investigation and analysis on digital evidence discovery through physical acquisition on smartphone. In *2015 World Congress on Internet Security (WorldCIS)*. IEEE, 132–138.

[14] Helmy Trisnasenjaya and Imam Riadi. 2019. 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* 8, 1 (2019), 89–98.

[15] Fu-Ching Tsai, En-Cih Chang, and Da-Yu Kao. 2018. WhatsApp network forensics: Discovering the communication payloads behind cybercriminals. In *2018 20th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 679–684.

[16] Rahul Vithala. 2019. Advantages and Disadvantages of WhatsApp. https://thetechhacker.com/2019/03/18/advantages-and-disadvantages-of-whatsapp/9

[17] WhatsApp. [n.d.]. *WhatsApp.* Retrieved May 24, 2021 from https://faq.whatsapp.com/general/payments/learn-more-about-participating-countries-and-supported-banks

[18] WhatsApp. 2021. *Om WhatsApp.* Retrieved May 24, 2021 from https://www.whatsapp.com/about/s

[19] Wikipedia. [n.d.]. *Extensible Messaging and Presence Protocol.* Retrieved April 26, 2021 from https://en.wikipedia.org/wiki/XMPP

[20] Wikipedia. [n.d.]. *Timeline of WhatsApp.* Retrieved April 26, 2021 from https://en.wikipedia.org/wiki/Timeline_of_WhatsApp

[21] Wikipedia. [n.d.]. *WhatsApp.* Retrieved May 24, 2021 from https://en.wikipedia.org/wiki/WhatsApp

[22] O. Yatskevich. 2019. How to Create a Chat App like WhatsApp. https://codetiburon.com/create-chat-app-like-whatsapp/

, ,

6 APPENDIX

A IMAGES & REVIEW RESPONDS

Content	Directory	File
contacts database	/data/data/ com.whatsapp/databases	wa.db (SQLite v.3)
chat database	/data/data/ com.whatsapp/databases	msgstore.db (SQLite v.3)

Fig. 2. Database files
[1]

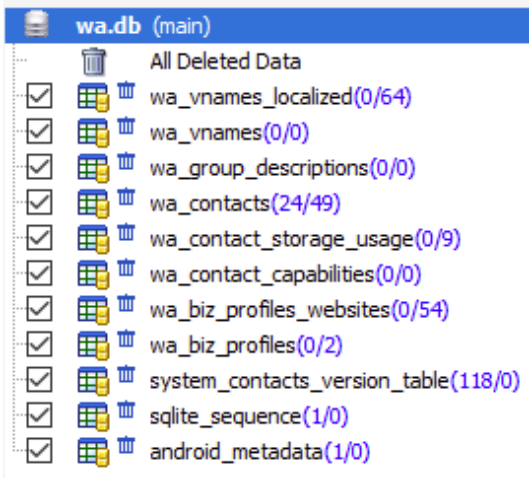

Fig. 3. Within wa.db
[8]

jid	is_wh...	status	status_timestamp	number	raw_contact_id	display_name
79[redacted]@s.whatsapp.net	1	Hey there! I am using WhatsApp.	1493537709000	+79[redacted]	73	Сер ватсап
79[redacted]@s.whatsapp.net	1	Hey there! I am using WhatsApp.	1511117556000	+79[redacted]	78	м2 ватс
37[redacted]2@s.whatsapp.net	1	Hey there! I am using WhatsApp.	1502981669000	+37[redacted]	80	анд ватс
98[redacted]2@s.whatsapp.net	1	Hey there! I am using WhatsApp.	1508090696000	+98[redacted]	125	Mohamed

Fig. 4. wa_contacts
[8]

docid	c0content
435	hi alex
436	plz call my person
437	hi
438	do you have btc and bch today ?
441	60k
442	??
443	can you deal today ?
445	money is ready
438	do you have btc and bch today ?
441	60k
442	??
443	can you deal today ?
445	money is ready

Fig. 5. message_fts_content
[8]

key_remote_jid	key_from_me	key_id	status	needs_push	data	timestamp	media_url
9[redacted]@s.whatsapp.net	0	3A803799543CC370399C	0	0	Plz call my person	1511770782000	
8[redacted]33@s.whatsapp.net	0	A5B5DC9927BFE2099AF41C64AF4A7F	0	0	hi	1511772438000	
8[redacted]33@s.whatsapp.net	0	3CF979D759CA3C6B210A352496ADC2	0	0	do you have BTC and BCH today?	1511772467000	
9[redacted]@s.whatsapp.net	0	call:15[redacted]	6	0		1511772745000	call_screen_presented
9[redacted]@s.whatsapp.net	0	8F9E8C26E3FAF517D717A20B401AE9	6	0		1511772745000	
9[redacted]@s.whatsapp.net	0	3AEC4DDBE88E62C56B78	0	0	60k	1511772762000	
7[redacted]@s.whatsapp.net	0	C1ECEF8A7189D81B8A7CA26E7E0644	0	0	??	1511773070000	
9[redacted]@s.whatsapp.net	0	3AE96FBFC0DA4EE264DC	0	0	Can you deal today?	1511773141000	
9[redacted]@s.whatsapp.net	0	call:15[redacted]	6	0		1511773697000	call_screen_presented
9[redacted]@s.whatsapp.net	0	3A8A511901CE30D53248	0	0	Money is ready	1511773705000	

Fig. 6. message_fts_content
[8]

	key_id	key_remote_jid	key_from_me	timestamp	received_timestamp	data
1	1329115800-1	39348[redacted]@s.whatsapp.net	0	1329116347000	1329116349643	Message 1
2	1329116349-1	39348[redacted]@s.whatsapp.net	1	1329116423505	1329116423532	Reply 1
3	1329115800-2	39348[redacted]@s.whatsapp.net	0	1329116791000	1329116793357	Message 2
4	1329116349-2	39348[redacted]@s.whatsapp.net	1	1329116941607	1329116941626	Reply 2

Fig. 7. Chat history
[1]

, ,

Fig. 8. Multimedia file exchange: sender side
[1]

Fig. 9. Multimedia file exchange: recipient side
[1]

Criteria	Open source tools		Commercial tools	
	TSK with Autopsy	***SIFT***	***MOBILedit! Forensic***	***Cellebrite's UFED Physical Analyzer***
Accuracy of Extraction	Less accurate	More accurate	Less accurate	More accurate
Advanced Image/Video Modules	Present	Present	Present	Present
Amount of community support available	Immense	Immense	Limited	Limited
Are results across multiple acquisitions consistent?	Mostly	Always	Mostly	Always
Availability of	Easily	Easily	Easily	Easily

Fig. 10. Comparison Open source vs Commercial tool [10]

Only part of the table is shown due to its length, the full result can be found in [10]