

A Comparative Study and Analysis of Forensic Artifacts of WhatsApp and Telegram on Android Devices

Rana Zaini Fathiyana ^{#1}, Yudiansyah ^{#2}, Nanang Cahyadi ^{#3}, Dinda Jaelani Hidayat ^{*4}

Institut Teknologi Telkom Jakarta

Jl. Daan Mogot KM.11 Kedaung Kali Angke, Cengkareng, Jakarta Barat, Indonesia

¹ ranazaini@ittelkom-jkt.ac.id

² yudiansyah@ittelkom-jkt.ac.id

³ nanangcahyadi@ittelkom-jkt.ac.id

** Badan Meteorologi Klimatologi dan Geofisika, Jakarta*

Jl. Angkasa 1 No.2, Gn. Sahari, Kec. Kemayoran, Jakarta Pusat, Indonesia

⁴ jaelanidinda@gmail.com

Abstract

Numerous instant messaging are available for mobile devices as a cheaper alternative over operator-based text messaging via SMS. Furthermore, instant messaging allow the user to exchange textual messages, images, audio, and videos. However, the ease offered by instant messaging also had a negative impact including making instant messaging as a criminal land. This paper focuses on conducting forensic data analysis of two popular instant messaging applications on Android smartphones; WhatsApp and Telegram. In this analysis, we use open-source tools and software applied on non-rooted Android devices. By using the result, an analyst will be able to read, and reconstruct the chronology of the messages and the list of contact and also know the difference in data structures obtained from these two instant messaging applications.

Keywords: Android Forensics, Instant Messaging Forensics, WhatsApp, Telegram

I. INTRODUCTION

THE growing number of mobile users worldwide followed by mobile app development that provides low-cost or free chat services as a cheaper alternative to operator-based text messaging via SMS. The use of this alternative service is broadly named instant messaging. Instant messaging is an online chat type that offers real-time text transmission over the internet [1, 2]. They provide a straightforward way to exchange text messages, graphics, video, audio messages, and emoticons or stickers. In addition, instant messaging also offers a variety of interesting features such as group chat, contact sharing, location sharing, and also file sharing [3].

Based on data from January 2022, WhatsApp is the most popular global mobile messenger application in the world with users over 2 million monthly active users. In terms of number of users, WhatsApp has increased significantly year by year [3]. Unlike WhatsApp, Telegram becomes a very popular instant messaging platform (in February 2016, the Telegram Messenger LLP company reported that there were 100,000,000 active users

per month, with 350,000 new users signing up per day [4]. As of the most recently reported period in [3], Telegram had 550 million global users as shown in Fig. 1.

The popularity of instant messaging services creates tremendous problems and challenges. One of them is to make instant messaging services a criminal land to launch its actions [5]. Such as cyberbullying, stalking sharing threatening, pornographic content, abuse, and other types of criminal acts using smartphones. In cases involving smartphone devices, instant messaging apps have the potential to be a source of evidentiary information in most investigations. So therefore, forensic analysis of this application is very important from the point of view of the investigation [6].

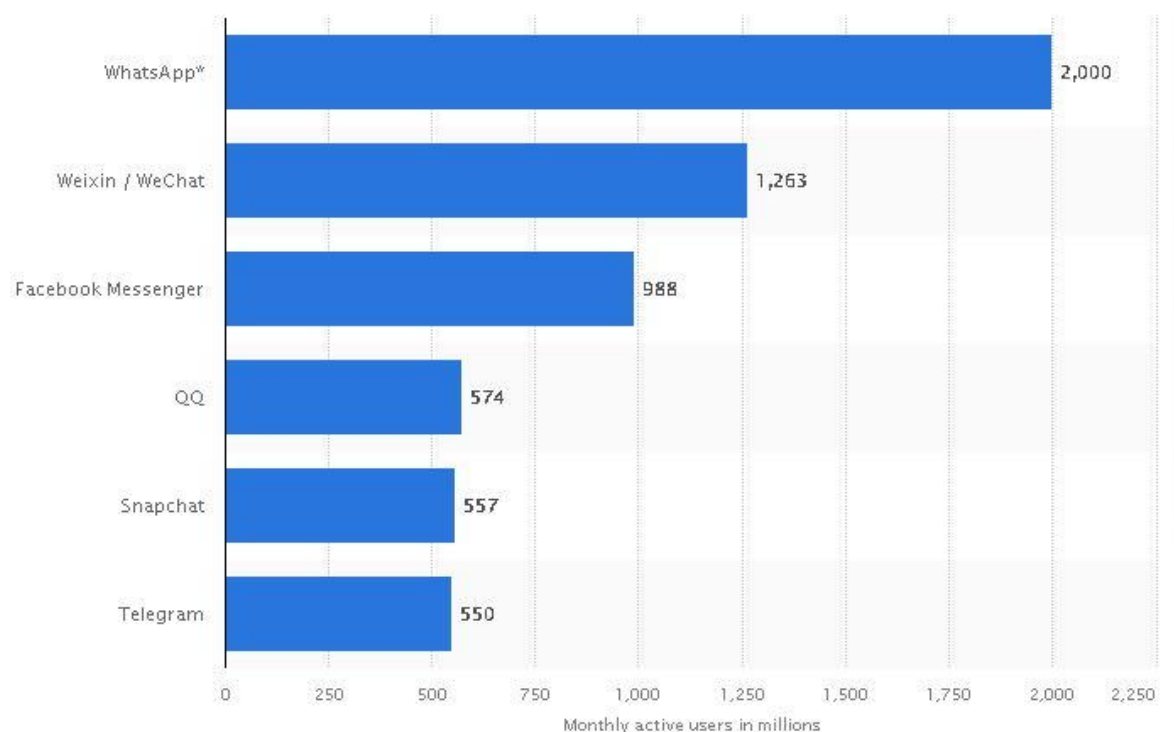


Fig. 1. Number of instant messaging user statistics [3]

Several previous works have been done on the same topic, as in literature [1, 2, 7, 8] but they present a methodology for the forensic analysis and artifacts generated on Android smartphones on instant messaging separately (especially WhatsApp and Telegram) so difficult when investigator will analyze the overall instant messaging installed on the smartphone. In this paper, we fill this gap by presenting a comparison and forensic evidence analysis of the data stored on WhatsApp and Telegram accessible on Android smartphones. These applications were chosen with their similar features and because both are the main targets for evil-doers and criminals to misuse these applications.

The rest of the paper is organized as follows: In Section 2 we describe related work, and review existing work, while in Section 3 we describe the methodology and the tools we use in our study. Then, in Section 4 we discuss the forensic analysis of WhatsApp and Telegram and then compare both of them as an experimental result. Finally, in Section 5 we conclude the paper and outline future research work.

II. LITERATURE REVIEW

The forensic analysis of instant messaging applications especially WhatsApp and Telegram on Android smartphones has been the subject of numerous works published in the literature. [1,7] focus on WhatsApp and [2, 8] on Telegram. By using the result [1] and [2] analysts will be able to reconstruct the list of contacts and the chronology of the messages that have been exchanged by the user. In [8] complete the [2] with the usage of the SHA-1 function is performed in this paper.

As [7] focus on the forensic analysis of WhatsApp, their work presents a step-by-step forensically sound procedure to extract WhatsApp conversations, which are by default encrypted, from a suspect or victim device and later decrypt it to convert them into human-readable formats which apply on non-rooted Android devices. The works of [7] are similar to ours, but for the implementation, we use a simpler tool to backup and retrieve a key file of WhatsApp by using the backup and restore tool provided by the OPPO smartphone (which is a scenario as evidence).

The works [9] and [10] focus on conducting forensic data analysis of two widely used instant messaging applications on Android smartphones: WhatsApp and Viber. As a differentiator, in our work, the subject of forensic analysis is WhatsApp and Telegram.

From all the literature, our contribution is to make a summary of the previous methodology by combining two methodologies in WhatsApp and Telegram in the simple way (non-rooted device). So hopefully, it will simplify the analysis of forensic instant messaging on android smartphones. In addition, we can know the difference in data structures obtained from these two instant messaging applications.

III. ANALYSIS AND METHODOLOGY

The study described in this paper has been performed by caring out a set of controlled experiments, referring to a usage scenario. After the experiment is done, the memory of the evidence device will be checked to identify, extract, and analyze the data generated by WhatsApp and Telegram installed on the Android smartphone.

The devices used in the forensic process are prepared to be able to perform the investigation. The device was configured with an operating system installed antivirus condition to prevent evidence contamination or deletion caused by virus attacks [11]. Used in this forensic analysis is OPPO F1s (A1601 32 GB) applied on non-rooted, Android version 5.1 (ColorOS), WhatsApp version 2.18.92, and Telegram 4.7.0.

A. *Software Tools*

1. WhatsApp Viewer (Version 1.11)
2. SQLite Database Browser (Version 3.10.1)
3. Backup and Restore (on OPPO smartphone device)

B. *Hardware Tools*

1. *Forensic Workstation* (Toshiba Satellite, Intel core i3, 4GB RAM, Windows 7 OS)
2. USB data cable
3. OPPO F1s (A1601 32 GB)

For this experiment used Android smartphones that are applied on non-rooted, is highly avoided to do permanent rooting because it is very risky to change the evidence [12].

C. Methodology

The first step to performing the acquisition of WhatsApp and Telegram is to perform a backup of internal and external memory data from both applications. To make backups using the backup and restore tool provided by the OPPO smartphone.

Choose to Create new backup – Applications then select WhatsApp and Telegram. After that to get the result from the backup prosses connect the mobile device to the forensic workstation using the appropriate data cable. The mobile device will display in My Computer as Portable Media Player as shown in Fig. 2. Browse the folder named Backup and then we can get the result as shown in Fig. 3 There are two folders to be analyzed further. WhatsApp and Telegram artifacts relevant to forensic investigations are analyzed within SQLite Database Browser.

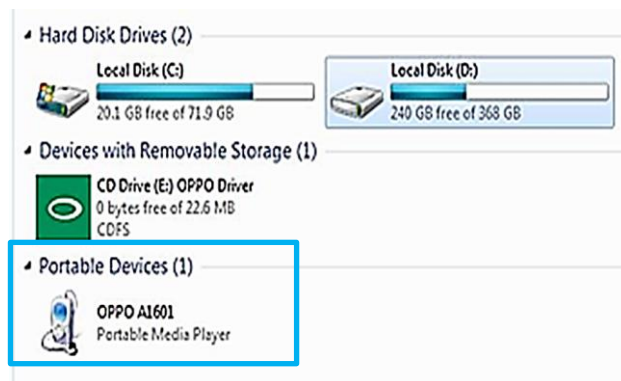


Fig. 2 Evidence device attached to forensic workstation



Fig. 3 Browse to App folders in Backup folder

In this way, the acquisition of the internal memory of that application is greatly simplified. However, if these files are checked only with SQLite Database Browser, we will get finite artifacts, because both data from this application are encrypted.

Since this database WhatsApp cannot be viewed directly (encrypted), so to access it, available some commercial tools such as Cellebrite and Oxygen Forensic but unfortunately, we did not have access to them. The alternative way that we choose to use open-source software is WhatsApp Viewer. To decrypt the WhatsApp database by using WhatsApp Viewer is needed key file of WhatsApp located in the folder com.whatsapp/files/key. From the acquisition process in step C, we have got the key file easily, without applying rooted on the device. But we did not find yet what kind of open source such as WhatsApp Viewer for Telegram. So, Telegram analysis is limited by using SQLite Database Browser.

IV. RESULTS AND DISCUSSION

A. Forensic Analysis of Database Schema of WhatsApp

WhatsApp has two different locations and names, namely “com.whatsapp” and “WhatsApp” folders. The folder location “com.whatsapp” is directly on directory /data/data/com.whatsapp/. Another folder named “WhatsApp” is located in external memory. Picture, audio, video files downloaded by the application were found in this folder.

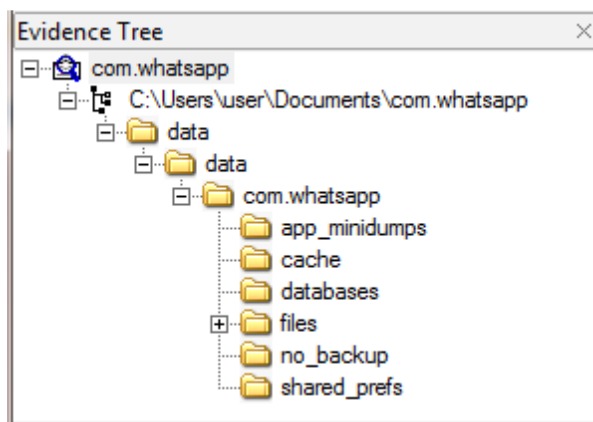


Fig. 4 Structure WhatsApp forensics analysis of com.whatsapp folder

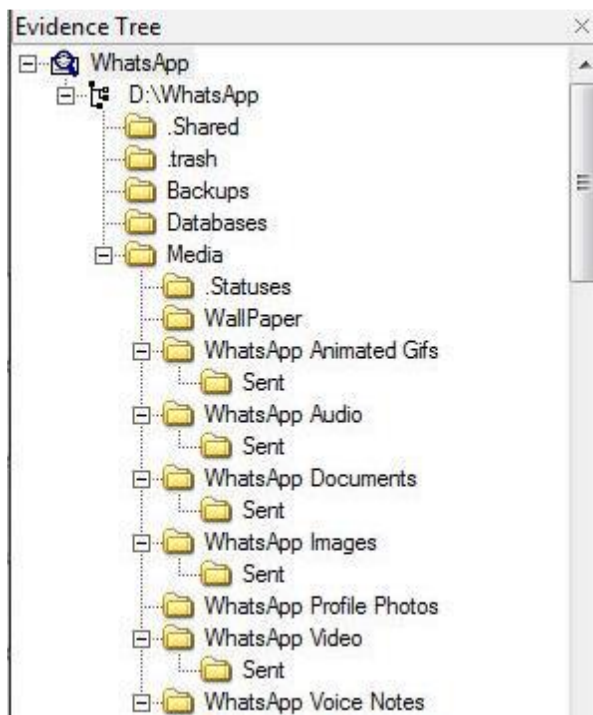


Fig. 5 Structure WhatsApp forensics analysis of WhatsApp folder

Forensic examination focus on folder “com.whatsapp” where there are msgstore.db and wa.db SQLite Databases. The msgstore.db contains details of any chat conversation between a user and their contacts. The wa.db stores information on the user’s contact list [10]. Both databases can be found under the

database folder at the following defined locations `wa.db: /data/data/com.whatsapp/databases` besides `msgstore.db: /data/data/com.whatsapp/databases`. Fig. 4 shows a snapshot of the structure of WhatsApp forensics analysis of `com.whatsapp` folder and Fig. 5 shows a structure of WhatsApp forensics analysis of the WhatsApp folder.

B. Forensic Analysis of Database Schema of Telegram

Telegram artifacts relevant to the forensic investigation are stored within SQLite Databases. Telegram artifacts on Android are stored found at the following locations:
`\data\data\org.telegram.messenger\files\cache4.db`

`cache4.db` databases store details on Telegram's user activities, contact information, messages exchange, sharing location/files, and delete chat [8]. Fig. 6 shows a snapshot of the structure of Telegram forensic analysis.

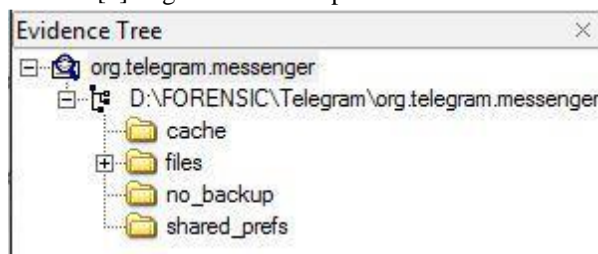


Fig. 6 Structure Telegram forensic analysis

C. Forensic Analysis of WhatsApp and Telegram

As discussed in section Methodology for the analysis of WhatsApp artifacts, we have used WhatsApp Viewer. As is already known that the `msgstore.db` is a database file containing conversations, while the `wa.db` contains the contact of the user WhatsApp including display name, phone number, and timestamp given upon registration. Both databases are required when using the WhatsApp Viewer with key files. Using WhatsApp Viewer, we can browse through available contacts and conversations between users of mobile devices and contacts [10].



Fig. 7 Provide the msgstore.db database and extracted key files

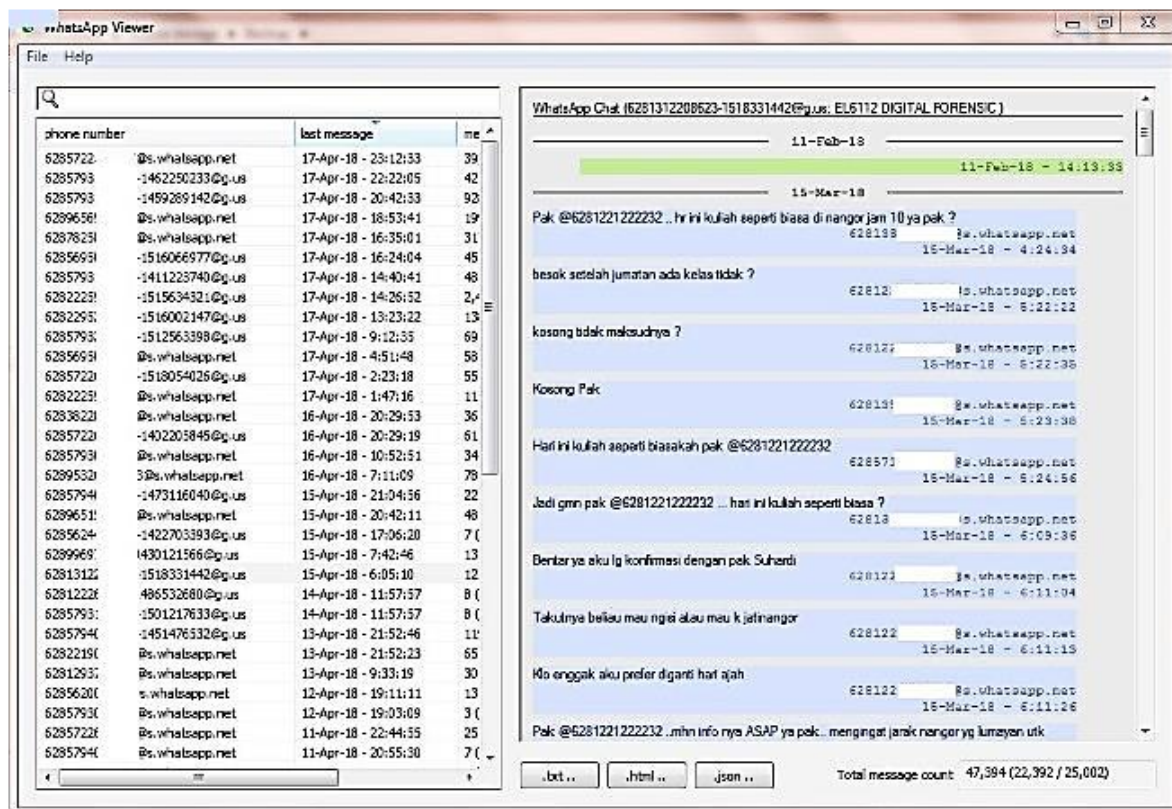
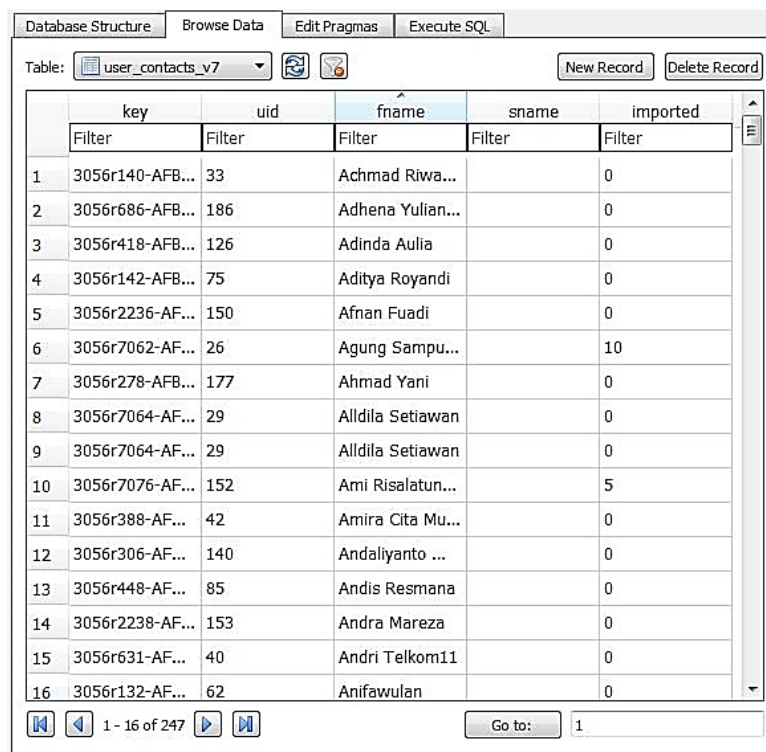


Fig. 8 Snapshot of WhatsApp Viewer

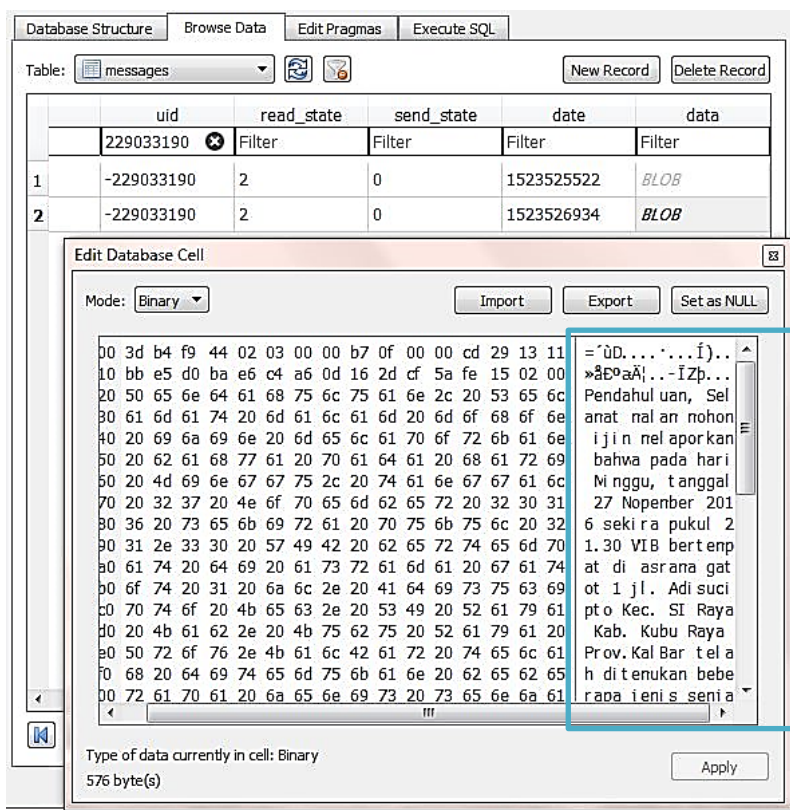
For the analysis of Telegram artifacts, we have used SQLite Database Browser. The unzipped folder `org.telegram.messenger` contains the database directly on `\data\data\org.telegram.messenger\files\cache4.db`. In the users, the table is shown `userID`, `name`, `status`, and `data`. Contact/users information not only exists in the users table, but also in `user_contact_v7` table (which are contained `userID`, `forename`, `surname`, and `imported`) and in a table of `user_phone_v7` (which are contained `phone number`, and `deleted`). We can see the table clearly as shown in Fig. 9.

Besides the three user tables, we can find out blocked contacts from the `blocked_users` table. We have also studied messages exchange. In this scenario, we created a group chat with `groupID 229033190`. All the information from the exchange of messages is stored on the `messages` table. Figure 10 is an example of the output text messages in `groupID 229033190` with the time it happened. From this result, we can see the plain text that is displayed in this table. So, it can be evidence to look at other evidence/chats for related that may have been used in cybercrime.



	key	uid	fname	sname	imported
1	3056r140-AFB...	33	Achmad Riwa...		0
2	3056r686-AFB...	186	Adhena Yulian...		0
3	3056r418-AFB...	126	Adinda Aulia		0
4	3056r142-AFB...	75	Aditya Royandi		0
5	3056r2236-AF...	150	Afnan Fuadi		0
6	3056r7062-AF...	26	Agung Sampu...		10
7	3056r278-AFB...	177	Ahmad Yani		0
8	3056r7064-AF...	29	Alldila Setiawan		0
9	3056r7064-AF...	29	Alldila Setiawan		0
10	3056r7076-AF...	152	Ami Risalatun...		5
11	3056r388-AF...	42	Amira Cita Mu...		0
12	3056r306-AF...	140	Andaliyanto ...		0
13	3056r448-AF...	85	Andis Resmana		0
14	3056r2238-AF...	153	Andra Mareza		0
15	3056r631-AF...	40	Andri Telkom11		0
16	3056r132-AF...	62	Anifawulan		0

Fig. 9 User database evidence in user_contacts_v7 table



	uid	read_state	send_state	date	data
1	-229033190	2	0	1523525522	BLOB
2	-229033190	2	0	1523526934	BLOB

Edit Database Cell

Mode: Binary

Import Export Set as NULL

```

00 3d b4 f9 44 02 03 00 00 b7 0f 00 00 cd 29 13 11
10 bb e5 d0 ba e6 c4 a6 0d 16 2d cf 5a fe 15 02 00
20 50 65 6e 64 61 68 75 6c 75 61 6e 2c 20 53 65 6c
30 61 6d 61 74 20 6d 61 6c 61 6d 20 6d 6f 68 6f 6e
40 20 69 6a 69 6e 20 6d 65 6c 61 70 6f 72 6b 61 6e
50 20 62 61 68 77 61 20 70 61 64 61 20 68 61 72 69
60 20 4d 69 6e 67 67 75 2c 20 74 61 6e 67 67 61 6c
70 20 32 37 20 4e 6f 70 65 6d 62 65 72 20 32 30 31
80 36 20 73 65 6b 69 72 61 20 70 75 6b 75 6c 20 32
90 31 2e 33 30 20 57 49 42 20 62 65 72 74 65 6d 70
a0 61 74 20 64 69 20 61 73 72 61 6d 61 20 67 61 74
b0 6f 74 20 31 20 6a 6c 2e 20 41 64 69 73 75 63 69
c0 70 74 6f 20 4b 65 63 2e 20 53 49 20 52 61 79 61
d0 20 4b 61 62 2e 20 4b 75 62 75 20 52 61 79 61 20
e0 50 72 6f 76 2e 4b 61 6c 42 61 72 20 74 65 6c 61
f0 68 20 64 69 74 65 6d 75 6b 61 6e 20 62 65 62 65
00 72 61 70 61 20 6a 65 6e 69 73 20 73 65 6e 6a 61

```

Type of data currently in cell: Binary
576 byte(s)

Apply

Fig. 10 Exchange of messages database evidence in messages table

D. Result of Research Findings and Forensic Analysis

With WhatsApp Viewer it is possible to extract and decode messages to reconstruct the chronology of the messages exchanged, determine when a message has been exchanged, the number of users involved in this conversation, and the data it carried. In the other words, digital artifacts from WhatsApp have been widely obtained. Otherwise, Telegram is limited to using only SQLite Database Browser so that the acquired digital artifacts are limited, not able to determine when a message has been exchanged.

V. CONCLUSION

This paper aimed to focus on finding and analyzing the artifacts from WhatsApp and Telegram on Android smartphones. In this paper, we performed a comparative study of database design in WhatsApp and Telegram. Intended to determine main artifacts easily from both instant messaging using available tools and software open source. These all research findings can help forensic investigators during any criminal incident and can be used as evidence in a court of law. But it was not focused on finding the artifacts if the data or application is deleted. And also the usage of any hash function is not performed in this paper. In the future, retrieving the artifacts of instant messaging after deleted data and strengthening evidence legitimization in court, using hash function analysis can be a part of our research scope.

REFERENCES

- [1] Cosimo Anglano, "Forensic analysis of whatsapp messenger on android smartphones", *Digital Investigation*, vol. 11, no. 3, pp. 201-213, 2014.
- [2] Cosimo Anglano, "Forensic analysis of telegram messenger on android smartphones", *Digital Investigation*, vol. 23, pp. 31-49, 2017.
- [3] statista, "Most popular global mobile messenger apps as of January 2022, based on number of monthly active users)", January 2022. [Online]. Available: <https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/>
- [4] Telegram Messenger LLP, Feb. 2016. 100,000,000 Monthly Active Users. Available: <https://telegram.org/blog/100-million>.
- [5] The United Nations Office on Drugs and Crime. Comprehensive Study on Cybercrime. Technical report, United Nations, Feb. 2013. Available at http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY/210213.pdf
- [6] Mohammad Iftexhar Husain, Ramalingam Sridhar (2010) iForensics: Forensic Analysis of Instant Messaging on Smart Phones http://link.springer.com/chapter/10.1007/978-3-642-115349_n_2?LI=true#
- [7] Gudipaty LP, Jhala KY (2015) WhatsApp Forensics: Decryption of Encrypted WhatsApp Databases on Non Rooted Android Devices. *J Inform Tech Softw Eng* 5: 147.
- [8] G. B. Satrya, P. T. Daely and M. A. Nugroho, "Digital forensic analysis of Telegram Messenger on Android devices," *2016 International Conference on Information & Communication Technology and Systems (ICTS)*, Surabaya, 2016, pp. 1-7.
- [9] Mahajan A., Dahiya M. and Sanghvi H. "Forensic Analysis of Instant Messenger Applications on Android Devices", *International Journal of Computer Applications* (0975 – 8887), April 2013, Vol. 68, No. 8.
- [10] AH Lone, FA Badroo, KR Chudhary, and A Khalique . "Implementation of Forensic Analysis Procedures for WhatsApp and Viber Android Applications", *International Journal of Computer Applications* (0975 – 8887). October 2015, Vol. 128, No. 12.
- [11] Hoog A (2011) *Android Forensics - Investigation Analysis & Mobile Security for Google Android*, Elsevier.
- [12] Shuaibu, M. Z. & Bala A., 2016. WhatsApp Forensics and Its Challenges for Android Smartphone. *A Global Journal of Advance Engineering Technology and Sciences*, (5) May 2016, pp. 68-75.