eJAICT

ISSN 2355 1771

JOURNAL OF APPLIED INFORMATION, COMMUNICATION AND TECHNOLOGY

Published by:
Research Center of Technology and Innovation
Academic Research and Community Services
Swiss German University

Forensic Analysis of Artifacts of Giant Instant Messaging “WhatsApp” in Android Smartphone

Hussein Abed Ghannam

Department of Information Technology, Swiss German University, Tangerang 15143, Indonesia

Article Information

Received: 1 August 2018
Accepted: 12 September 2018
Published: 3 October 2018
DOI: 10.33555/ejaict.v5i2.55

Corresponding Author:

Hussein Abed Ghannam
Email: enghag2012@gmail.com

ISSN 2355-1771

ABSTRACT

WhatsApp is a giant mobile instant message IM application with over 1billion users. The huge usage of IM like WhatsApp through giant smart phone “Android” makes the digital forensic researchers to study deeply. The artefacts left behind in the smartphone play very important role in any electronic crime, or any terror attack. “WhatsApp” as a biggest IM in the globe is considered to be very important resource for information gathering about any digital crime. Recently, end-to-end encryption and many other important features were added and no device forensic analysis or network forensic analysis studies have been performed to the time of writing this paper. This paper explains how can we able to extract the Crypt Key of “WhatsApp” to decrypt the databases and extract precious artefacts resides in the android system without rooting the device. Artefacts that extracted from the last version of WhatsApp have been analysed and correlate to give new valuable evidentiary traces that help in investigating. Many hardware and software tools for mobile and forensics are used to collect as much digital evidence as possible from persistent storage on android device. Some of these tools are commercial like UFED Cellebrite and Andriller, and other are open source tools such as autopsy, adb, WhatCrypt. All of these tools that forensically sound accompanied this research to discover a lot of artefacts resides in android internal storage in WhatsApp application.

Keywords: *WhatsApp; Android; Android Forensic Analysis; Artifacts; Encryption; Instant Message*

1. Introduction

1.1. Background

WhatsApp is the most widely instant message used in the globe boasting over 1 billion user, it was founded in 2009 by Brian Acton and Jan Koum and bought by Facebook for 19 billion $ in 19 Feb 2014, while the android that developed by Google is the most successful and famous mobile operating system in the world wide with an 80% share of the global smartphone market (www.telegraph.co.uk). Besides the prediction for smartphone will be 2.9 billion by the end 2020 (https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide.) Due to the huge popularity of android smart phone and IM services especially WhatsApp, people used to use IM in their daily life in many activities, from the other side organized criminals or terrorist groups also uses the same technology for illicit purposes, either they use it to contact the potential victim or to escape from the interception. Therefore, the right way of analysis of WhatsApp artefacts either from the mobile device side or network has the interest of digital forensic companies and experts. Android forensic is relatively new field in digital forensic, while processes of extraction the data from mobile devices in general are acquired by commercial tools such as Cellebrite UFED, MSAB XRY, and Oxygen Forensic Suite, the output of extracted data from these commercial tools are in different formats. Across the low enforcement and civil investigation, there are variety of mobile devices to be examined, and the use of multiple tools (open source tools), methods and process may be required to extract and analyse data from mobile.

1.2. Significance

The current version of WhatsApp in android is 2.17.393 enriched with many new features. For the digital forensic practitioners, some of these features considered as challenges have to be solved. Such feature like end-to-end encryption released in March 31, 2016 and developed in collaboration with Open Whisper System (WhatsApp Encryption Overview). This end-to-end encryption protocol is designed to prevent third parties and WhatsApp from having plaintext access to messages or calls. Many researchers published many papers before the releasing of end-to-end encryption like (Karpisek, et al., 2015) (Karpisek, F., Baggili, I., Breitinger, F.) for forensic analysis for artefacts of calls. The information resides in the instant messages (e.g. WhatsApp) in mobile devices can answer about important questions in any investigation process. The need for mobile forensic analysis increases as shown by the figure1 the number of mobile devices presented for analysis in between 2004-2014 of South Australia Office SAP, this is provided by (Darren Quick et al., 2016) (Quick, D. and Kim-Choo, K.R., 2016).

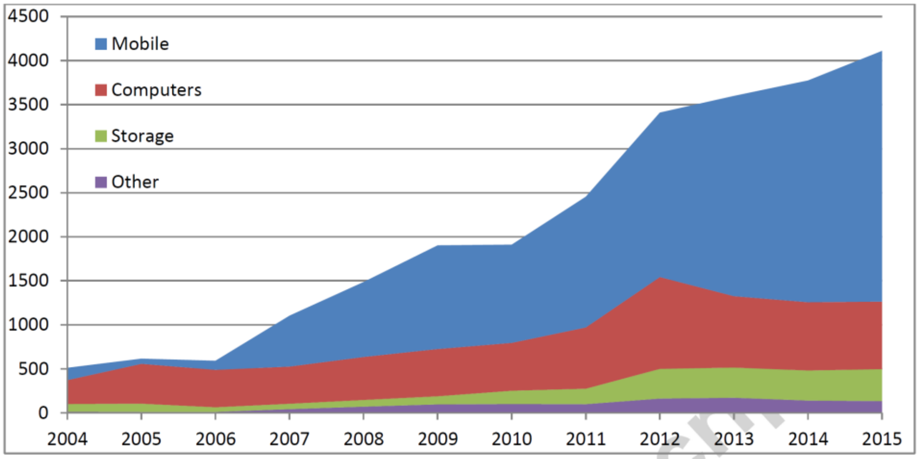


Figure 1: SAPOL ECS - Devices presented for analysis per Year (2004-2014).

1.3. Research Problem

In the very increasingly growth of smartphone market, and with same side of huge depending from people on the instant message in their daily life, fast update of instant messages IM improve the features of the application and attract participants to continue using their product. On the other side most of these features will create a big challenge for the practitioners and experts that work in digital forensic. Many researches have been conducted to collect data from old version of WhatsApp application. After the release of new versions of WhatsApp, many security features appeared to create a challenge for mobile forensic practitioners to collect information and evidences resides in internal storage. This research suggested new different methods in extracting the data from WhatsApp android. WhatsApp databases was encrypted with new technique and save in SD (new with crypt12) in a form (e.g.msgstore.db.crypt12 for chat content).

1.4. Research Objectives

We are going to acquire and analyse the artefacts of last release of WhatsApp application running in android system. Many techniques and tools are used in this research to satisfy the following targets:

1- Logical extraction the content of encrypted database of WhatsApp IM running in android smartphone.
2- Analyze and correlate the artifacts produced from database to produce new valuable evidentiary traces that help in investigating.

1.5. Research Question:

What are techniques, methods and tools in an android forensic to retrieve the artifacts from WhatsApp Instant Message IM application running in android smartphone?

2. Related Work

Mobile forensic is a very important branch of digital forensic, as defined by NIST National Institute of Standards and Technology, “mobile device forensic is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods” (Ayers, R., Brothers, S., Jansen, W., 2014). The researches that have been conducted on the forensics of WhatsApp either focus on the data that WhatsApp stores or Many researchers published papers about this topic, (Lessard & Kessler, 2010) (Lessard, J., & Kessler, G., 2010) used many techniques, tools and methods to retrieve and recovery data from android device. Tools such dd, adb, FTK Forensic Tool Kit and Cellebrite were used in his research to recover a lot of evidence even passwords, google maps, and others. Since the Mobile devices probably have more information that can be linked to an individual than most computers.

There are many researches and papers written before this research treated the mobile forensic analysis of old release of WhatsApp application in android system, (Anglano, 2014) (Anglano, C., 2014). who performed a deep mobile forensic analysis of WhatsApp on Android devices. In his research, he didn’t content with the artefacts generated by WhatsApp but also he provided some methods to reconstruct the contact list and chronology of the chat messages have been exchanged between the users. From (Mahajan, et al., 2013) (*Mahajan, A., Dahiya, M.S. and Sanghvi, H.P.,* 2013), he mainly used a commercial tool UFED to analyse physically the WhatsApp and Viber instant messages. Many of the artefacts were extracted from many models of android devices such as chat messages, storage location, timestamps, and file names sent or received from android devices, database files (msgstore.db and wa.db). All of these extractions were done by Mahajan in old release of WhatsApp, our analysis in this research will be in the latest version and release of WhatsApp that has a lot of update features that need deep analysis in extracting the artefacts. While in (Thakur, 2013) (Thakur, N.S., 2013). research, he extracted and analysed the volatile memory as well (RAM of the android device) in order to get the chat sessions of the deleted data. He used also commercial tool like UFED and open source tool WhatsApp Xtract to retrieve evidentiary artefacts from android. At that time, the WhatsApp Database Encryption Project had a known vulnerability in the android implementation of the AES cipher and (Thakur 2013) (Thakur, N.S., 2013). used Francesco Picasso tool to decrypt and organize SQLite database of WhatsApp. For the current release of WhatsApp, the strength of encryption is big and needs more effort to export the key of encryption with different ways, the one that we did in this research. (F. Karpisek et.al, 2015) studied WhatsApp network communication to decrypt network traffic and obtain the forensic artefacts such as WhatsApp phone number, WhatsApp server IP, phone call establishment, phone call termination, phone call voice codec and relay server IP addresses. As we know, more features are added to WhatsApp from the time of conducting (F. Karpisek et.al, 2015) research, our research conducted new experiments on new protocols used by WhatsApp on android system.

Rooting the android device is really trade-off between knowing deeply about the directory structure of files and the data stored in RAM of android device and (Vidas, et al., 2011) (Vidas T., Zhang C., Christin N., 2011). who considered rooting same meaning as exploiting a security vulnerability and may alters portions of the device that may store user data. (Vidas, et al., 2011) suggest different methods in acquiring the image of internal storage of android that accepted by (ACPO, 2007) (“ACPO 2007”) and forensically sound. In the network forensic analysis part, (Walnycky et al., DFRWS 2015 USA) (http://library.college.police.uk/docs/acpo/police-use-of-digital-images-2007.pdf.) opted 20 of instant message/social messaging applications. The team discussed about security perspective regarding most of these IMs, at the same time the investigator can get a lot of digital evidence from the artefacts either by android forensic way or by network forensic. “Datapp” is their own tool to automate the process of capturing the data in real time.

3. Methodology

3.1. Overview

The main purpose of this research is find techniques, tools and methods to retrieve the artifacts of the last release of WhatsApp running in the android OS. This research treated device forensic of the artifacts that resides in the WhatsApp in the internal storage. The experiments were conducted in a lab containing different hardware and software commercial and open source tools. These experiments focused in retrieving the artifacts of last version of WhatsApp installed in android system, including key encryption, contacts, messages, photos, videos, and many others. WhatsApp artifacts were taken by logical and physical acquisitions for the android system. Fig.2 shows the methodology of this research to acquire and analyze the artefacts generated by WhatsApp on android smart phone by using two kinds of acquisition logical and physical.

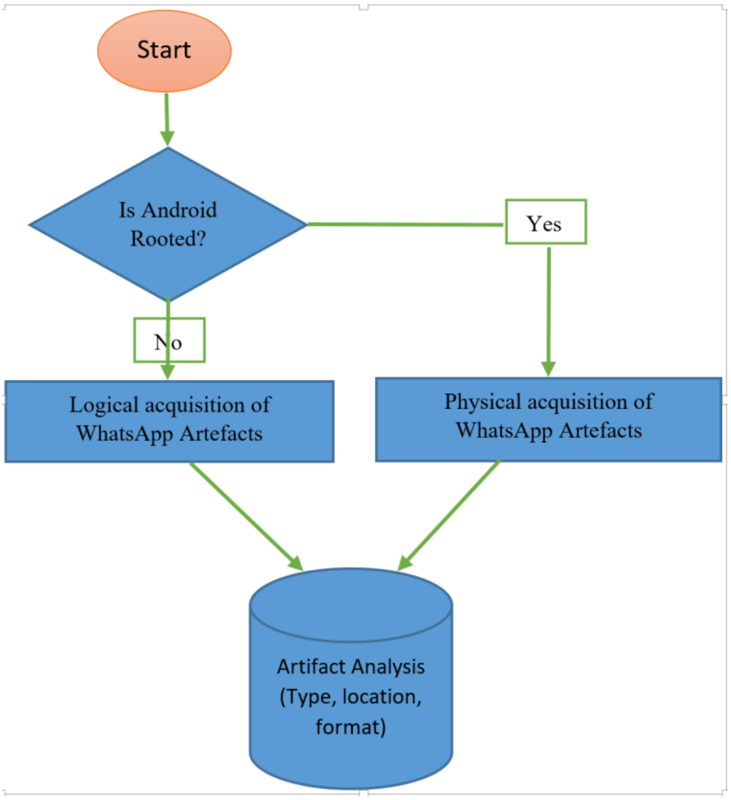

Start
Is Android Rooted?
Yes
No
Logical acquisition of WhatsApp Artefacts
Physical acquisition of WhatsApp Artefacts
Artifact Analysis (Type, location, format)

Fig. 2. Methodology Design of Acquiring and Analysis of WhatsApp Artefacts.

3.2. Requirements for Experiments

Prior to start the experiments, the forensic work station was installed and configured. This environment was isolated from any internet and network connection to preserve the digital evidence from any outer interaction. Hereby the list of hardware and software tools used in this research experiments shown in Table 1.

Table 1: Hardware and Software tools needed to extract and analyze WA logically and physically

Hardware / Software	Role of Each Item in Experiment / Details
Android phone	Samsung Galaxy note II of model number GT-N7100 (Experiment)
USB data cables	Connect the android device to Forensic Workstation
WhatsApp application	running in android.
WhatCrypt application	Extracting the crypt key of WA from android
Android studio	package of tools to run adb and avdmanager and others.
SQLite Database Recovery v1.2	From systools software (Walnycky, et al., 2015) to read .db files in WA artefacts.
Andriller	Commercial mobile forensic tool to run physical acquisition.
Cellebrite UFED	Commercial mobile forensic tool to run physical acquisition and recover deleted messages.

3.3. Experimental study

3.3.1. Logical extraction of WA databases

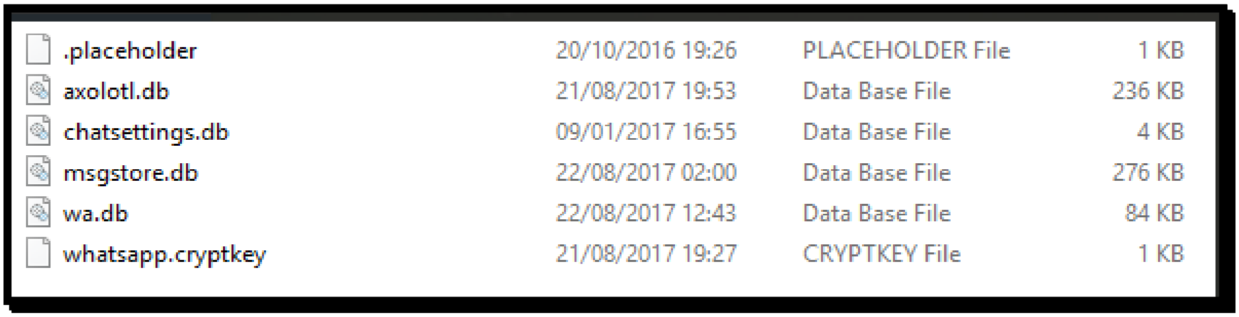
The research will cover the traces of WhatsApp application in the persistent storage (internal memory) of android device without expanding to volatile memory of android. In the experiment we used mobile phone of type Samsung Galaxy note II of model number GT-N7100 with android version 4.4.2 (Codename KitKat) (https://www.systoolsgroup.com/sqlite-database-recovery.html) that shown in Table1. Then we installed the latest release of WhatsApp with Version 2.17.286 - at the timing of writing these lines (https://developer.android.com/about/dashboards/index.html). I prepared two android devices to communicate between each other and make one of them as our target (Galaxy one), I began our search by sending some chat messages, files, images, contacts, locations, and others. WhatsApp stores the user data (which our target) in SQLite database called *msgstore.db* and *wa.db*. Without rooting the android device, we can get backed up WhatsApp folder that stored in SD card, this mainly contains three sub folders like below:

/sdcard/WhatsApp/Databases
/sdcard/WhatsApp/Media
/sdcard/WhatsApp/ProfilePictures

Moreover, the decryption of WhatsApp Crypt12 is possible without rooting the android device by getting Crypt key of database, because the last release of WhatsApp stored is totally different with old versions that was vulnerable and has weaknesses in encryption mechanism. The WhatsApp Database Encryption Project (https://www.whatsapp.com/android/.) , implies that the same AES with a 192-bit encryption key (346a23652a46392b4d73257c67317e352e3372482177652c) is being used for all WhatsApp installations on the Android platform. By using the tool "*Whatcrypt*" (Cortjens, D., Spruyt, A., and Wieringa, W. F. C.), script by "TripCode" we can extract the WhatsApp key file and DB on android 4.0+. The database resides in the form of encrypted file on the android external storage SD card at path:

/sdcard/WhatsApp/Databases/msgstore.db.crypt12

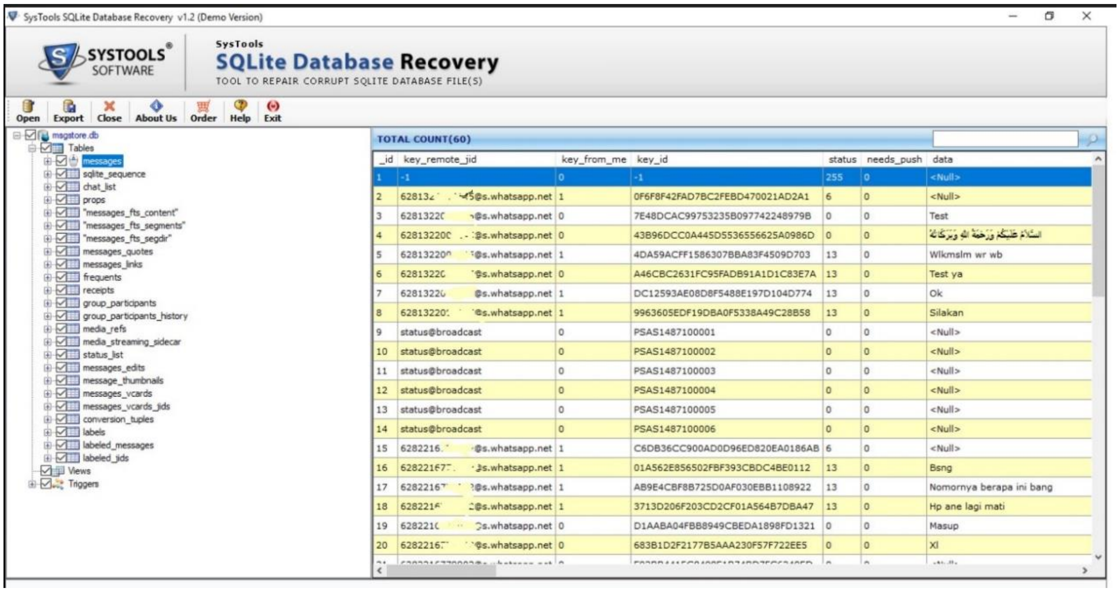
Even though android device is not rooted yet, the tool "Whatcrypt" still can retrieve many artefacts of WhatsApp stored in android by using "Crypt Key Extractor" tool that is available for both Linux and windows version. For windows you can find WhatsAppKeyDBExtractor.ps1 and WhatsAppKeyDBExtractor.bat for extracting the key file. After extracting the key file, it should be uploaded with the msgtore.db.crypt12 to Whatcrypt to be decrypted the msgtore.db as shown in fig.3.



.placeholder	20/10/2016 19:26	PLACEHOLDER File	1 KB
axolotl.db	21/08/2017 19:53	Data Base File	236 KB
chatsettings.db	09/01/2017 16:55	Data Base File	4 KB
msgstore.db	22/08/2017 02:00	Data Base File	276 KB
wa.db	22/08/2017 12:43	Data Base File	84 KB
whatsapp.cryptkey	21/08/2017 19:27	CRYPTKEY File	1 KB

Fig.3: The results of WA databased after decrypting by WhatCrypt.

Then we opened all the DB content or msgstore.db with any database viewer, in our case we used the tool "SQLite Database Recovery" to examine the databases maintained by android's WhatsApp as shown in fig.4. It is forcibly recommended for privacy and security perspectives to download the "apk" tool "WhatCrypt" to use it offline and not used the online site.



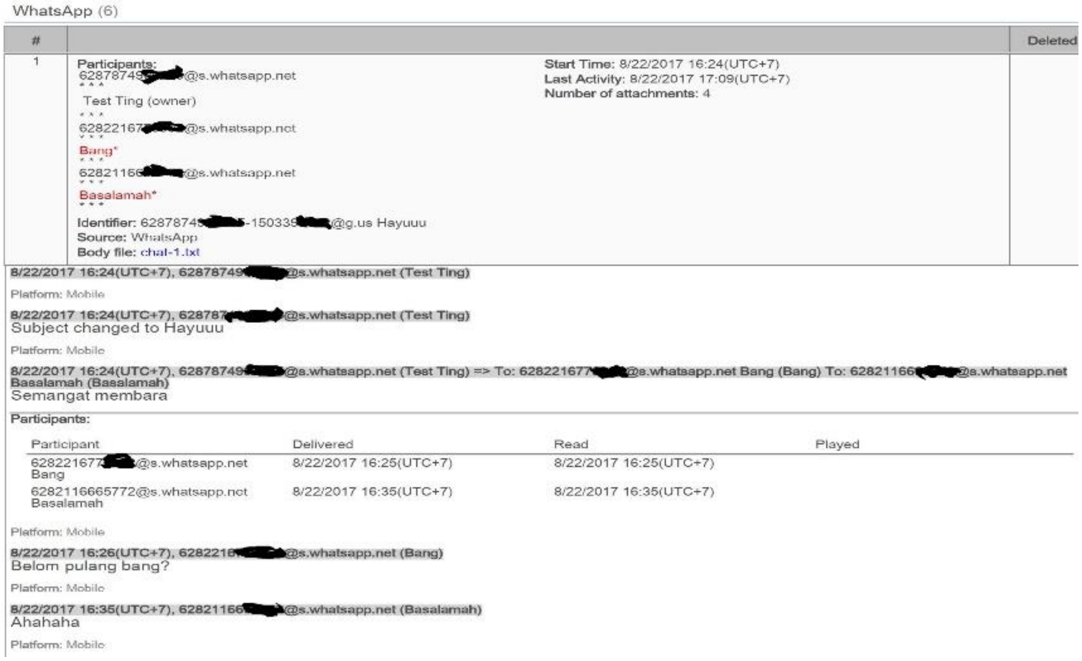
TOTAL COUNT(60)

_id	key_remote_jid	key_from_me	key_id	status	needs_push	data
1	-1	0	-1	255	0	<Null>
2	62813[redacted]@s.whatsapp.net	1	0F6F8F42FAD7BC2FEBD470021AD2A1	6	0	<Null>
3	6281322[redacted]@s.whatsapp.net	0	7E48DCAC99753235B097742248979B	0	0	Test
4	6281322[redacted]@s.whatsapp.net	0	43B96DCC0A445D5536556625A0986D	0	0	السَّلَامُ عَلَيْكُمْ وَرَحْمَةُ اللهِ وَبَرَكَاتُهُ
5	6281322[redacted]@s.whatsapp.net	1	4DA59ACFF1586307BBA83F4509D703	13	0	Wlkmslm wr wb
6	6281322[redacted]@s.whatsapp.net	0	A46CBC2631FC95FADB91A1D1C83E7A	13	0	Test ya
7	6281322[redacted]@s.whatsapp.net	1	DC12593AE08D8F5488E197D104D774	13	0	Ok
8	6281322[redacted]@s.whatsapp.net	1	9963605EDF19DBA0F5338A49C28B58	13	0	Silakan
9	status@broadcast	0	PSAS1487100001	0	0	<Null>
10	status@broadcast	0	PSAS1487100002	0	0	<Null>
11	status@broadcast	0	PSAS1487100003	0	0	<Null>
12	status@broadcast	0	PSAS1487100004	0	0	<Null>
13	status@broadcast	0	PSAS1487100005	0	0	<Null>
14	status@broadcast	0	PSAS1487100006	0	0	<Null>
15	6282216[redacted]@s.whatsapp.net	1	C6DB36CC900AD0D96ED820EA0186AB	6	0	<Null>
16	6282216[redacted]s.whatsapp.net	1	01A562E856502FBF393CBDC4BE0112	13	0	Bsng
17	6282216[redacted]@s.whatsapp.net	1	AB9E4CBF8B725D0AF030EBB1108922	13	0	Nomornya berapa ini bang
18	628221[redacted]@s.whatsapp.net	1	3713D206F203CD2CF01A564B7DBA47	13	0	Hp ane lagi mati
19	628221[redacted]s.whatsapp.net	0	D1AABA04FBB8949CBEDA1898FD1321	0	0	Masup
20	6282216[redacted]@s.whatsapp.net	0	683B1D2F2177B5AAA230F57F722EE5	0	0	Xl

Fig.3: Exporting the SQLite database (msgstore.db) to view the artefacts.

3.3.2. Physical extraction by Cellbrite UFED

WhatsApp users may delete various information that considered as a digital evidence such as main database, contacts, individual messages or entire messages. It is known in forensic domain that these deleted artefacts still resides in an area called unallocated data. These portions of data can be recovered by many ways, one of the best commercial tools is UFED cellbrite that we used to recover deleted chat as shown in fig.4.


WhatsApp (6)

#		Deleted
1	**Participants:** 62878749[redacted]@s.whatsapp.net * * * Test Ting (owner) * * * 6282216[redacted]@s.whatsapp.net * * * Bang* * * * 628211[redacted]@s.whatsapp.net * * * Basalamah* * * * **Identifier:** 6287874[redacted]-150339[redacted]@g.us Hayuuu **Source:** WhatsApp **Body file:** chat-1.txt **Start Time:** 8/22/2017 16:24(UTC+7) **Last Activity:** 8/22/2017 17:09(UTC+7) **Number of attachments:** 4	

8/22/2017 16:24(UTC+7), 62878749[redacted]@s.whatsapp.net (Test Ting)

Platform: Mobile

8/22/2017 16:24(UTC+7), 628787[redacted]@s.whatsapp.net (Test Ting)
Subject changed to Hayuuu

Platform: Mobile

8/22/2017 16:24(UTC+7), 62878749[redacted]@s.whatsapp.net (Test Ting) => To: 62822167[redacted]@s.whatsapp.net Bang (Bang) To: 6282116[redacted]@s.whatsapp.net Basalamah (Basalamah)
Semangat membara

Participants:

Participant	Delivered	Read	Played
62822167[redacted]@s.whatsapp.net Bang	8/22/2017 16:25(UTC+7)	8/22/2017 16:25(UTC+7)	
6282116665772@s.whatsapp.net Basalamah	8/22/2017 16:35(UTC+7)	8/22/2017 16:35(UTC+7)	

Platform: Mobile

8/22/2017 16:26(UTC+7), 6282216[redacted]@s.whatsapp.net (Bang)
Belom pulang bang?

Platform: Mobile

8/22/2017 16:35(UTC+7), 6282116[redacted]@s.whatsapp.net (Basalamah)
Ahahaha

Platform: Mobile

Fig.4: Deleted individual chat (red colour) recovered by UFED physical extraction.

4. Findings and Results

In this part of paper, we will present the findings and results of the artifacts by making direct comparison between the methods that we apply in section 3. These results depicted in table2 shown below.

Table 2: Comparison of Artefacts of WA discovered by different tools.

	Internal storage+ No rooting with adb	**Internal storage (SDcard) + No rooting with adb + WhatCrypt**	**Internal storage + rooting + UFED Cellbrite**
Msgstore.db	Found encrypted	Found	Found
Wa.db	Not found	Found	Found
Phone number	Found if db decrypted	Found	Found
Messages	Found if db decrypted	Found	Found
Media Files	Found	found	found
Contact Cards	Found if db decrypted	Found	Found
Location	Found if db decrypted	Found	found
SQL queries	Found if db decrypted	Found	Found
Profile pictures	Not found	Not found	found
Logs	Not found	Not found	Found
Directory Structure	Not found	Found	Found
Deleted Messages	Not found	Not found	Found
Deleted Media Files	Not found	Not found	Found

WhatsApp is rich in feature that provide the users with many functionalities that should be in point of interest to forensic analysis. Most of these functionalities that we already found displayed in table2. For the manual extraction that appeared in column1 we connected to physical device by using android debugging bridge "adb" and extract most of artefacts files that still encrypted (Appendix A). In another experiment we use another tool called WhatCrypt to decrypt the results that we got from the first experiment and we get new results in Column2 in Table2 and details of these experiments shown in Appendix B.

5. Conclusion

In this paper, we have presented some methods and techniques to acquire and analyze logically the artifacts of WhatsApp running in android smartphone. The experiments was done on a real android smart phone and not use virtualized one. We identify most of the artifacts left by WhatsApp in internal storage or persistent memory of the device. In future many works can be done regarding applying the same experiments in different mobile operating system like IOS or Windows Phone. Besides, there are still some experiments can be done on the volatile memory RAM of the device to acquire more artifacts.

References

“ACPO 2007” Practice Advice of Association of Chief Police Officers”.

Anglano, C. (2014). Forensic analysis of WhatsApp messenger on Android smartphones.

Ayers, R., Brothers, S., Jansen, W. (2014) Guidelines on mobile device forensics. NIST Special Publication 800.

Cortjens, D., Spruyt, A., and Wieringa, W. F. C. "WhatsApp Database Encryption Project Report."
http://whatcrypt.com/

https://developer.android.com/about/dashboards/index.html.

http://library.college.police.uk/docs/acpo/police-use-of-digital-images-2007.pdf.
http://www.telegraph.co.uk/technology/google/11676110/Android-chief-downplays-importance-of-operating-system.html.

https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide.

https://www.systoolsgroup.com/sqlite-database-recovery.html

https://www.whatsapp.com/android/.

Karpisek, F., Baggili, I., Breitinger, F. WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages.

Lessard, J., & Kessler, G. (2010) Android forensics: Simplifying cell phone examinations.

Mahajan, A., Dahiya, M.S. and Sanghvi, H.P. (2013) "Forensic Analysis of Instant Messenger Applications on Android Devices".

Quick, D. and Kim-Choo, K.R. (2016). Pervasive Social Networking Forensics: Intelligence and Evidence from Mobile Device Extracts.

Thakur, N.S., (2013). “Forensic Analysis of WhatsApp on Android Smartphones”,. University Of New Orleans.

Vidas T., Zhang C., Christin N., (2011). “Toward a general collection methodology for Android devices”,

Walnycky, D., Baggili, I., Marrington, A., Moore J., Breitinger, F. (2015). “Network and device forensic analysis of Android”.

WhatsApp Encryption Overview, Technical white paper, July 6 2017, originally published April 5, 2016.