Forensic Acquisition of Data from a Crypt 12 Encrypted Database of Whatsapp

John Alhassan
Federal University of Technology Minna
59 PUBLICATIONS **149** CITATIONS
SEE PROFILE

Bilkisu Abubakar
Federal University of Technology Minna
1 PUBLICATION **2** CITATIONS
SEE PROFILE

Morufu Olalere
Federal University of Technology Minna
23 PUBLICATIONS **90** CITATIONS
SEE PROFILE

Shafi'i Muhammad Abdulhamid
Federal University of Technology Minna
109 PUBLICATIONS **1,484** CITATIONS
SEE PROFILE

Forensic Acquisition of Data from a Crypt 12 Encrypted Database of Whatsapp

John K Alhassan, Bilikisu Abubakar, Morufu Olalere, Shafi'i Muhammad Abdulhamid and Suleiman Ahmad
Department of Cyber Security, Federal University of Technology, Minna, Nigeria.
jkalhassan@futminna.edu.ng, bilkisu.abu@futminna.edu.ng, lerejide@futminna.edu.ng,
shafii.abdulhamid@futminna.edu.ng, ahmads@futminna.edu.ng

ABSTRACT
Mobile phone devices have become popular among every age and social grouping in every society and are utilised by lots of people for different purposes. As the design of Mobile phones are continually evolving due to advancement in present technologies, applications that run on them are also being updated to fully utilise features on new devices. Due to the flexibility and portability coupled with applications that make communication easy and accessible, these devices are now mostly used to perform e-transactions, social networking and even criminal activities. One of such applications is WhatsApp which over various versions have tried to maintain the confidentiality and integrity of messages sent and received using WhatsApp. Securing of data from Criminals or unauthorized users called for constant updating of the encryption scheme of the SQLite database which is usually saved on the memory of the device on which it is installed. Over many updates of WhatsApp, the encryption has been changed from db.crypt, db.crypt5, db.crypt7, db.crypt8 to db.crypt12. There is need for forensic expert to constantly update their knowledge so as to get the needed information from the database. This study presents a forensic process of extracting WhatsApp data from db.crypt12, which is the latest SQLite Database encryption used by WhatsApp to secure stored communication data. The steps involve using some open source tools that can be downloaded for free on the internet.

Keywords*: Forensic Analysis, Whatsapp, Mobile Phones, Database*

1. INTRODUCTION

Mobile phone devices are found everywhere in our society, utilized by lots of people for different purposes. The flexibility and portability incorporated into the design of Mobile phones differ and are continually changing as present technologies advance and new technologies are brought in. Smart phone devices are mostly used to perform e-transactions, used for social networking and even criminal activities.

Most at times mobile phones are used to commit offences, the users delete the information that can be linked to an offence so that evidence cannot be found against them. Mobile phone forensics analysis is an effective means of gathering trails of digital data for criminal evidence, which is much hard to remove (Taylor et al., 2012 & Abdulhamid et al, 2017).

There are different kinds of mobile phone forensics which includes recorded mobile phone conversation, mobile texts messages, digital photos, emails, contacts no. lists and mobile digital video recordings (Walnycky et al., 2015). When evidence is gathered for legal uses, this has to be preserved and kept to avoid damage or removal of essential digital materials through systems built up for data extraction from mobile phone. Usually, mobile phone forensics are used in digital data recovery of deleted contents. These can help the legal teams or law enforcement agency, resulting in legal evidence production and presentation.

Wikipedia describes WhatsApp Messenger “as a patented, different-platform, encrypted instant message client for smartphones. Internet connection is required to send messages, documents, PDF files, GIF images, video and audio messages to other individuals utilizing standard cell phone numbers”. The company WhatsApp Incorporated, was established in 2009 by the founder Brian Acton and Jan Koum, who were one-time workers in Yahoo! In February 2014, months after valuation of capital financing round at $1.5 billion, WhatsApp was worth $1.5B. Facebook informed it was buying WhatsApp for $19 billion, its most enormous procurement to date ("Facebook to Acquire WhatsApp," 2014)

WhatsApp was the major globally common messaging app, in August 2014 it has over 600 million active users Olsen (2014). WhatsApp made over seven hundred (700) million active users monthly and more than thirty (30) billion messages where being sent every day Kim (2015) in January of 2015. In April of 2015, the application had over eight hundred (800) million active users. These large numbers of users has made WhatsApp one of the most suitable digital evidence gathering platforms compared to Over-The-Top services like Skype and other short messaging service options. By September of 2015, the users had increased to nine (900) hundred million, and by February of 2016 it had increased to over one billion. (Statt and Nick, 2016).

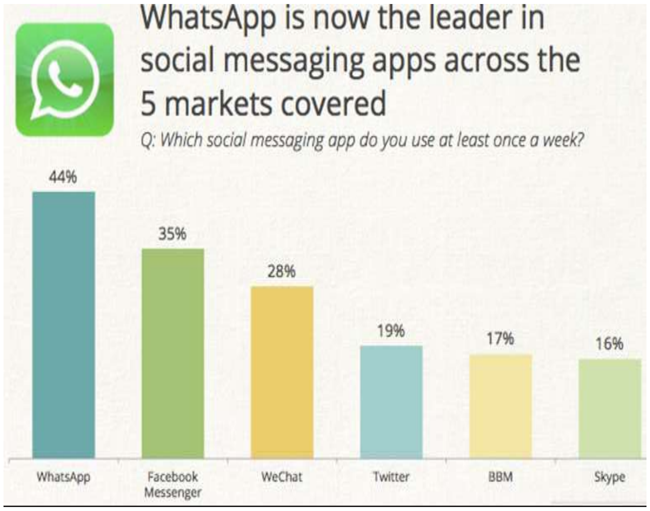


Figure 1: global snapshot of popularity among 6 social networking apps (Source: WhatsApp Forensics and Its Challenges for Android Smartphone)

In February 2016, WhatsApp made users of about one billion, making it the most popular messaging application (Statt and Nick, 2016).

WHATSAPP APPLICATION BEFORE NOW AND TODAY

WhatsApp data is kept in the Internal Memory of a mobile phone. After it has been installed, it automatically operates with the phone's contacts indicating individuals who are using WhatsApp already. Whenever a mobile phone device which has the WhatsApp application installed on it is turned on, the “com.whatsapp” procedure obtains a prompt to start the 'External Media Manage' and 'Message Service' services that functions behind the scene on the mobile phone till the mobile phone is turned on.

A. Before Now

Messages exchanged on earlier versions of WhatsApp were kept in 'msgstore.db' which is a SQLite databases. However, in early versions, security scientists discovered that WhatsApp chat records were vulnerable, because the database file which keeps the chat records was not encrypted. This can result to easy accessibility of the entire conversation chat details such as contacts, images, videos, and so forth. When this information reaches the internet, security investigators began to research with WhatsApp database (msgstore.db) in an attempt to recover the conversations from the chat option even the deleted ones. Only for WhatsApp to respond soon and came up with an encryption mechanism to safeguard its database (Sahu, 2014).

B. Today

Presently, according to WhatsApp officials they are considering the conversation database security in a very important manner, at present WhatsApp database encryption have custom Advanced Encryption Standard (AES) encryption algorithm with over 192-bit encryption key primarily employed for WhatsApp Android Platform. Thus the previous file *msgstore.db* is now converted to *msgstore.db.crypt*, *msgstore.db.crypt*5,*msgstore.db.crypt*7, *msgstore.db.crypt*8 and finally *msgstore.db.crypt*12 which is encrypted by AES algorithm with 256-bit key (Ibrahim, 2016)

2. REVIEW OF RELATED WORKS

Mobile device forensics is the skill of acquiring digital prove from a mobile device under forensically sound conditions using accepted methods. It is an evolving specialty in the field of digital forensics (Lohiya, John, and Pooja Shah, 2015). The goal of mobile forensics is the act of employing sound methodologies for obtaining data contained inside the internal memory of a mobile device and related media giving the capability to accurately report one’s discoveries.

Abidin (2015) forensically analyzed Instagram, a third-party application installed on mobile phones. The author conducted forensic investigation on Instagram which is a popular social networking application to find out if activities carried out with smartphone’s social networking applications are stored in the internal storage of the mobile device and what sort of forensic data can be obtained or found in the device. The methodology used in this study could not show strong evidence that the exhibit (i.e mobile phone) was used to send or transfer images to and from Instagram. The authors’ analysis of the Instagram account discovered in the smartphone was unable to prove that the device was used at any time to login as administrator. Details such as registered email and password were not found in the device.

In the research work by Walnycky, Baggili, Marrington, Moore, & Breitinger (2015) titled “Network and device forensic analysis of Android social-messaging applications” acquired forensic data to analyze the network traffic of 20 widely used instant messaging applications on the Android platform and also device-stored data. The authors rebuilt some residual content from sixteen (16) out of twenty (20) mobile applications that was examined; pointing to an inadequate security requirements and privacy standard used by the various applications but may be interpreted as positive for evidence gathering intent by forensic professionals.

Al Mutawa, Baggili, & Marrington (2012) in a paper titled "Forensic analysis of social networking applications on mobile devices" carried out forensic analysis on three most utilized social networking mobile apps on smart phones: Facebook, Myspace and Twitter. They carried out a test on three widely used smartphones: Android phones, BlackBerrys and iPhones. The tests include installation of these applications on selected devices, carrying on similar user actions on each application. The authors acquired a forensically good logical image of all the devices used, then performed a manual analysis of each of the logical image. These analyses were intended at detect if activities performed by these applications were kept on the device's internal memory. Their results showed that chat messages from android phone were recovered. However, no traces could be found on BlackBerry devices.

Karpisek, Baggili, & Breitinger (2015) carried out a research to decrypt and understand WhatsApp call signaling messages. The authors described how network traffic was decrypted to acquire forensic artefact's that pertain to a new feature for placing call which includes WhatsApp audio codec (Opus), WhatsApp phone numbers, WhatsApp call duration, WhatsApp server IPs, and WhatsApp's call termination. The tools and methods used to decrypt the traffic as well as their findings with regard to the WhatsApp signalling communications was explained.

Anglano, Canonico, & Guazzone (2016) present an approach focuses on presenting forensic analysis of the artefacts generated on Android smartphones by Chat Secure, a secure Instant Messaging application that provides strong encryption for transmitted and locally-stored data to ensure the privacy of its users. The methodology used was based on the use of emulated devices that provides a very high degree of reproducibility of the results, and validated the results it yields against those obtained from real smartphones.

Mahajan, Dahiya, & Sanghvi (2013) present a paper titled "Forensic Analysis of Instant Messenger Applications on Android Devices" carried out a forensic analysis of two popular instant messaging applications (IMs) on an Android smart phones: WhatsApp and Viber, with the objective of finding out what data or information can be extracted from the internal memory of the device's for instant messengers. A Universal Forensic Extraction Device (UFED) Classic Ultimate (V 1.8.0.0) physical analyzer was used to analyze the two applications. In the instance of WhatsApp, they found chat message artefacts, sent file names, send and received timestamps were obtained. However, it was not possible to determine the locations were those files are stored. While manually testing WhatsApp application after the File System was Extracted, database files 'msgstore.db and wa.db' were discovered with chat sessions information. The authors did not analyze the RAM for any WhatsApp application data residues or attempt recovery of erased data.

In a paper presented by Sahu, (2014) "An Analysis of WhatsApp Forensics in Android Smartphones" the focus was on performing forensic analysis by gathering helpful forensic data from WhatsApp and from corresponding mobile applications installed on an Android smartphone. The method the author applied was that a Python tool was used to decrypt and read the encrypted database with the latest version of WhatsApp 2.11. 186. However, after phone reset, artefacts became irretrievable and erased data irrecoverable.

Forensic Analysis Android Smartphones with WhatsApp application installed was considered by Thakur (2013). The approach focuses on WhatsApp application. The author describe how forensic experts can acquire helpful forensic information from android devices running WhatsApp and similar applications installed on a mobile device running Android. The author performed a real-time analysis on an Android smartphone to acquire user interaction details from the application. The evidence collection process concentrated on getting and analyzing of user application data from the device's external storage and the RAM of an Android device. Although the tool the authors used could extract user data from RAM their work could not interpret data extracted from RAM into human readable form. Also, the tools they used were not customized to display user specific information, the tool could only highlight three aspects of user data that is to say messages they exchanged, contact numbers of users along with database queries which disclose the basic structure of database for WhatsApp.

In this work, a forensic method of extracting data from a crypt12 encrypted WhatsApp database stored on an android mobile form is presented furthering research in the area.

3. RESEARCH METHODOLOGY

The main aim of this study is to forensically extract data stored by WhatsApp with a crypt 12 SQLite database on android mobile device. The goal of the research was reached successfully.

A. *Performing Forensics Analysis on WhatsApp Data Using Android Smartphone*

To perform forensic analysis for the purpose of recovering evidence from a crypt12 encrypted database on an android mobile device, a set of tools/software's are required. These tools are

TABLE I. LIST OF HARDWARE AND SOFT WARE USED FOR FORENSIC ANALYSIS

Requirements	***Specification***
Android Smart phone	Infinix hot
WhatsApp Application	Version 2.17.2
Forensic WorkStation	HP Envy intel core i7
Omni crypt	Version 3.0.2
WhatsApp extract	Version 2.2
SQlite DB Browser	Version 3.9.1

B. Preparing the Android device under forensic investigation.

The first step to perform acquisition of WhatsApp database file is turning off the mobile or switching it to flight mode to ensure that it is disconnected from all external networks.

The omni crypt android application discussed in section 3.2is then installed on the device. The app is free for down load on android playstore at https://play.google.com/store/apps/details?id=com.omnicrypt&hl=en.

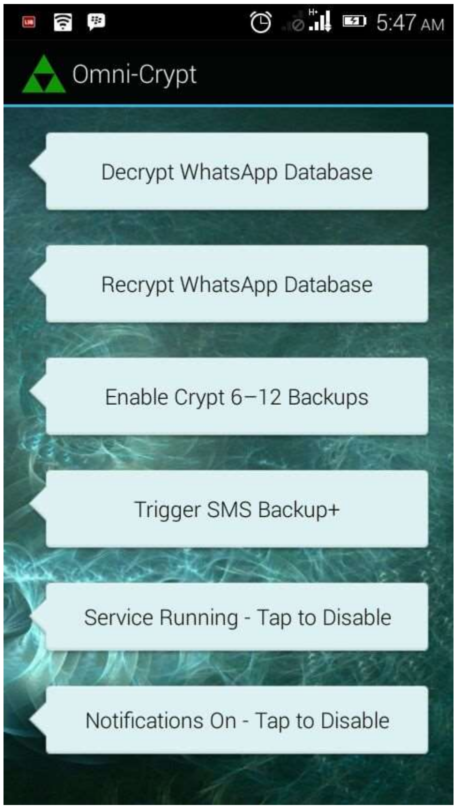

5:47 AM
Omni-Crypt
Decrypt WhatsApp Database
Recrypt WhatsApp Database
Enable Crypt 6–12 Backups
Trigger SMS Backup+
Service Running - Tap to Disable
Notifications On - Tap to Disable

Figure 2: Omni crypt app user interface installed on the device

The database must be decrypted on the device to the legacy Cypt encryption which the WhatsApp xtract tool is able to extract a SQLite readable database from. To achieve this, tab on the third option on the Omni crypt app interface "enable crypt 6 – 12 backups". You will receive a pop up alert saying it has been enabled.

This allows the Omni Crypt app to locate the WhatsApp database folder on the SD card (default memory where WhatsApp is installed). If the device does not contain an SD card, Omni crypt will detect the default memory (Phone storage). You may now proceed to tap on "decrypt WhatsApp Database"

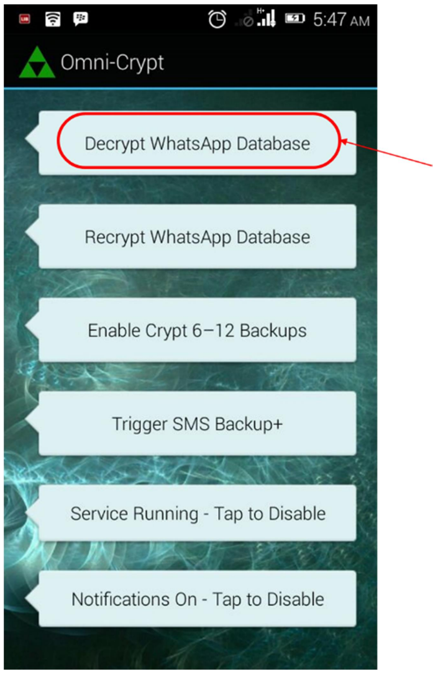
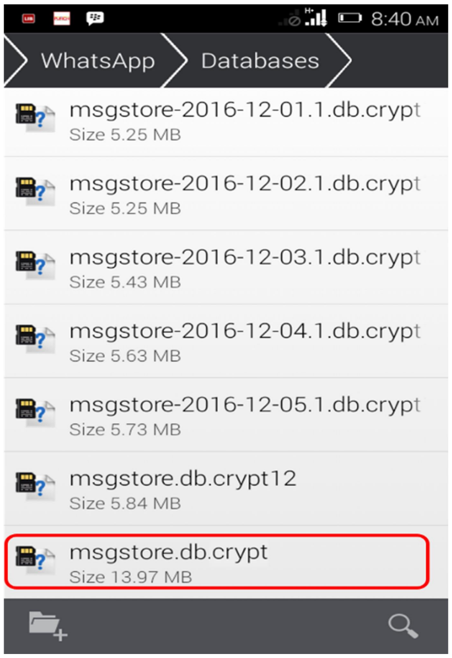

5:47 AM
Omni-Crypt
Decrypt WhatsApp Database
Recrypt WhatsApp Database
Enable Crypt 6–12 Backups
Trigger SMS Backup+
Service Running - Tap to Disable
Notifications On - Tap to Disable

Figure 3: Decrypting the WhatsApp database

On taping the option on Figure 2, Omni crypt decrypts the last backed up database from. crypt12 (Msgstore.db.crypt12) to legacy .crypt (Msgstore.db.crypt) shown in Figure 3 using a key stored on the device which it finds and uses to create a copy of the database with that encryption. This is the copy of the database that will be copied to the forensic workstation for decryption to an unencrypted database that can be opened and viewed by the SQLite DB browser.



msgstore-2016-12-01.1.db.crypt
Size 5.25 MB

msgstore-2016-12-02.1.db.crypt
Size 5.25 MB

msgstore-2016-12-03.1.db.crypt
Size 5.43 MB

msgstore-2016-12-04.1.db.crypt
Size 5.63 MB

msgstore-2016-12-05.1.db.crypt
Size 5.73 MB

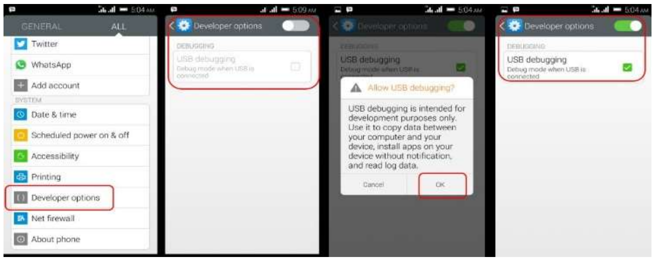
msgstore.db.crypt12
Size 5.84 MB

msgstore.db.crypt
Size 13.97 MB

Figure 4: .crypt database created from .crypt12 database using Omni.

C. *Retrieving the database from the Android device under forensic investigation.*

The device must now be placed on developer's mode by navigating to Settings > About > Software Information > More. Then tap the devices "Build number" seven times to enable Developer options. Return to Settings menu and you will see "Developer options" there. Tap on it and turn on USB Debugging from the menu on the next screen. (Figure 5).



USB debugging is intended for development purposes only. Use it to copy data between your computer and your device, install apps on your device without notification, and read log data.

Figure 5: Enabling USB debugging on Android device.

Using an appropriate USB cable, connect the mobile device to the forensic workstation. On connecting successfully, the mobile device will display in My Computer as Portable Media Player.

Double click on the mobile device and Browse to the folder named "WhatsApp" and then browse in a folder named Databases. (Figures 6). Since these databases are encrypted and cannot be viewed directly, we require a cipher key that is stored inside the RAM of the mobile device. However, before copying the database from the device onto the work station, click on internal memory folder and browse to WhatsApp folder to find the database folder which contains WhatsApp database file as shown in figure 7

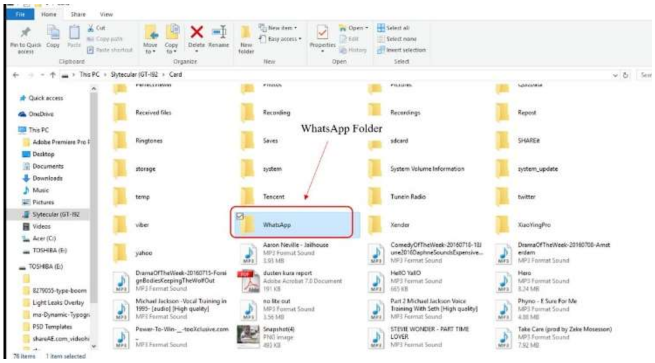
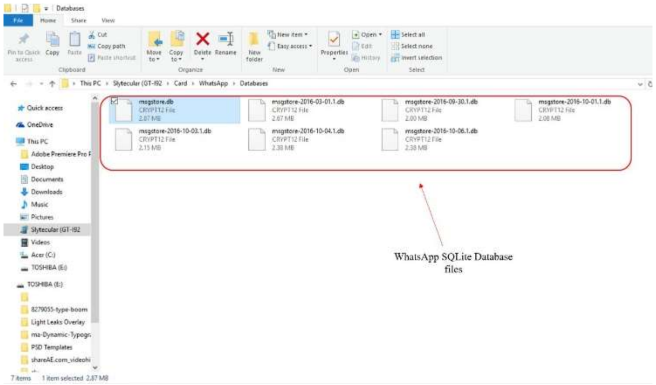


Figure 6: WhatsApp folder in SD card



This PC > Slytecular (GT-I92 > Card > WhatsApp > Databases

msgstore.db
CRYPT12 File
2.87 MB

msgstore-2016-03-01.1.db
CRYPT12 File
2.67 MB

msgstore-2016-09-30.1.db
CRYPT12 File
2.00 MB

msgstore-2016-10-01.1.db
CRYPT12 File
2.08 MB

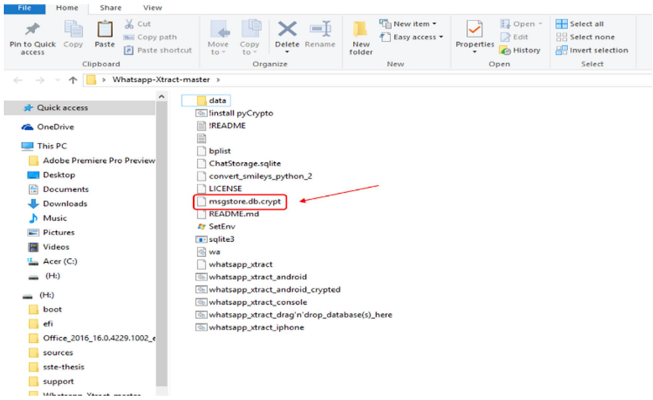
msgstore-2016-10-03.1.db
CRYPT12 File
2.15 MB

msgstore-2016-10-04.1.db
CRYPT12 File
2.38 MB

msgstore-2016-10-06.1.db
CRYPT12 File
2.38 MB

Figure 7: WhatsApp database from the mobile device under investigation**.**

The next step is the database file retrieved from the android device under investigation should be placed in the WhatsApp Xtract folder (figure 8).

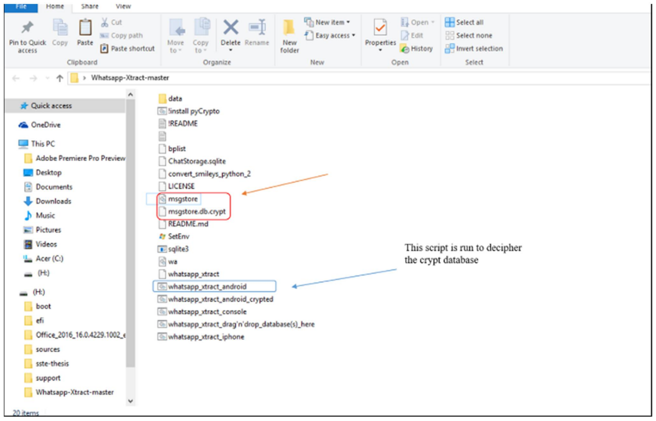


Whatsapp-Xtract-master >

data
!install pyCrypto
!README
bplist
ChatStorage.sqlite
convert_smileys_python_2
LICENSE
msgstore.db.crypt
README.md
SetEnv
sqlite3
wa
whatsapp_xtract
whatsapp_xtract_android
whatsapp_xtract_android_crypted
whatsapp_xtract_console
whatsapp_xtract_drag'n'drop_database(s)_here
whatsapp_xtract_iphone

Figure 8: Database file placed in WhatsApp Xtract

The extract tool is run using Whatsapp_extract_andriod script to decipher the crypt database as shown in figure 9.

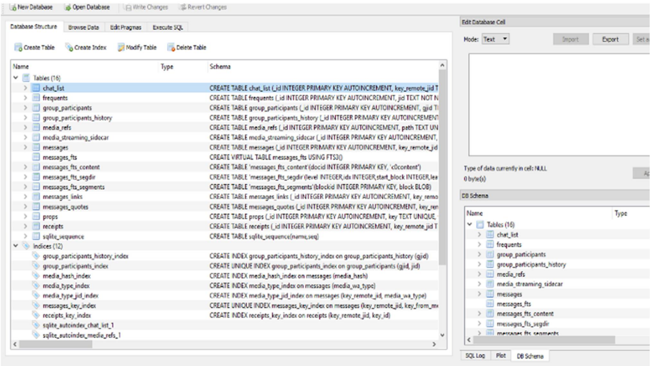


data
!install pyCrypto
!README
bplist
ChatStorage.sqlite
convert_smileys_python_2
LICENSE
msgstore
msgstore.db.crypt
README.md
SetEnv
sqlite3
wa
whatsapp_xtract
whatsapp_xtract_android
whatsapp_xtract_android_crypted
whatsapp_xtract_console
whatsapp_xtract_drag'n'drop_database(s)_here
whatsapp_xtract_iphone

This script is run to decipher the crypt database

Figure 9: The database file after running the extract tool

The database can now be viewed with the DB browser tool.



Name	Type	Schema
Tables (16)		
chat_list		CREATE TABLE chat_list (_id INTEGER PRIMARY KEY AUTOINCREMENT, key_remote_jid T
frequents		CREATE TABLE frequents (_id INTEGER PRIMARY KEY AUTOINCREMENT, jid TEXT NOT N
group_participants		CREATE TABLE group_participants (_id INTEGER PRIMARY KEY AUTOINCREMENT, gjid T
group_participants_history		CREATE TABLE group_participants_history (_id INTEGER PRIMARY KEY AUTOINCREMENT
media_refs		CREATE TABLE media_refs (_id INTEGER PRIMARY KEY AUTOINCREMENT, path TEXT UN
media_streaming_sidecar		CREATE TABLE media_streaming_sidecar (_id INTEGER PRIMARY KEY AUTOINCREMENT,
messages		CREATE TABLE messages (_id INTEGER PRIMARY KEY AUTOINCREMENT, key_remote_jid
messages_fts		CREATE VIRTUAL TABLE messages_fts USING FTS3()
messages_fts_content		CREATE TABLE 'messages_fts_content'(docid INTEGER PRIMARY KEY, 'c0content')
messages_fts_segdir		CREATE TABLE 'messages_fts_segdir'(level INTEGER,idx INTEGER,start_block INTEGER,lea
messages_fts_segments		CREATE TABLE 'messages_fts_segments'(blockid INTEGER PRIMARY KEY, block BLOB)
messages_links		CREATE TABLE messages_links (_id INTEGER PRIMARY KEY AUTOINCREMENT, key_remo
messages_quotes		CREATE TABLE messages_quotes (_id INTEGER PRIMARY KEY AUTOINCREMENT, key_rem
props		CREATE TABLE props (_id INTEGER PRIMARY KEY AUTOINCREMENT, key TEXT UNIQUE,
receipts		CREATE TABLE receipts (_id INTEGER PRIMARY KEY AUTOINCREMENT, key_remote_jid T
sqlite_sequence		CREATE TABLE sqlite_sequence(name,seq)
Indices (12)		
group_participants_history_index		CREATE INDEX group_participants_history_index on group_participants_history (gjid)
group_participants_index		CREATE UNIQUE INDEX group_participants_index on group_participants (gjid, jid)
media_hash_index		CREATE INDEX media_hash_index on messages (media_hash)
media_type_index		CREATE INDEX media_type_index on messages (media_wa_type)
media_type_jid_index		CREATE INDEX media_type_jid_index on messages (key_remote_jid, media_wa_type)
messages_key_index		CREATE UNIQUE INDEX messages_key_index on messages (key_remote_jid, key_from_me
receipts_key_index		CREATE INDEX receipts_key_index on receipts (key_remote_jid, key_id)
sqlite_autoindex_chat_list_1		
sqlite_autoindex_media_refs_1		

Figure 10: Database tables after decryption and viewing with the DB browser

Figure 10 shows the tables on the database that was decrypted from the android device under forensic investigation. There are 16 tables on the database with 16 indices. The tables are chat_list,frequents,group_participants,group_participants_history,media_refs,media_streaming_sidecar,messages,messages_fts, messages_fts_content, etc.

4. RESULTS AND DISCUSSION

Prior to applying the methodology employed in this study, it was impossible to read or write into the SQLite database stored on the android device SD card. This is now possible as shown in Figure 10. The resultant database store (msgstore.db) can be explored using the DB browser for SQLite Database by opening the database with the software tool. This can be done by clicking the open database tab and navigating to where the database is stored on the workstation. Once this is done, the browser displays a list of tables present on the database store which include the chat_list, frequents, group_participants, group_participants_history, media_refs, media_streaming_sidecar, messages, messages_fts, messages_fts_content and other tables. Tables can be switched by clicking on the drop down menu of the on the browse data tab and selecting the desired table (Figure 11)

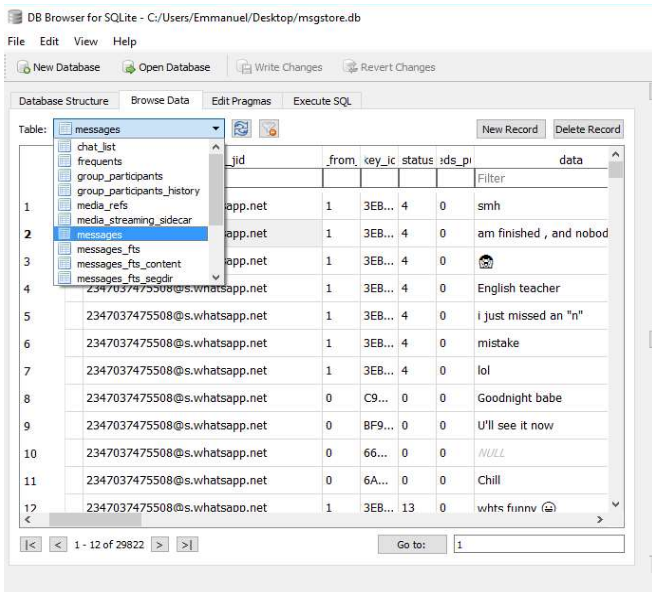


Table: messages

chat_list
frequents
group_participants
group_participants_history
media_refs
media_streaming_sidecar
messages
messages_fts
messages_fts_content
messages_fts_segdir

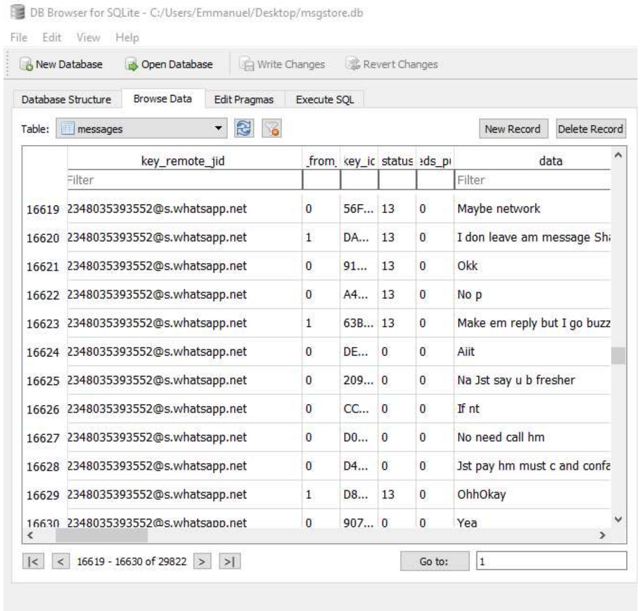
	_jid	_from_	key_ic	status	ːds_pı	data
						Filter
1	app.net	1	3EB...	4	0	smh
2	app.net	1	3EB...	4	0	am finished , and nobod
3	app.net	1	3EB...	4	0	😱
4	2347037475508@s.whatsapp.net	1	3EB...	4	0	English teacher
5	2347037475508@s.whatsapp.net	1	3EB...	4	0	i just missed an "n"
6	2347037475508@s.whatsapp.net	1	3EB...	4	0	mistake
7	2347037475508@s.whatsapp.net	1	3EB...	4	0	lol
8	2347037475508@s.whatsapp.net	0	C9...	0	0	Goodnight babe
9	2347037475508@s.whatsapp.net	0	BF9...	0	0	U'll see it now
10	2347037475508@s.whatsapp.net	0	66...	0	0	NULL
11	2347037475508@s.whatsapp.net	0	6A...	0	0	Chill
12	2347037475508@s.whatsapp.net	1	3EB...	13	0	whts funny 😀

|< < 1 - 12 of 29822 > >|

Go to: 1

Figure 11: Switching database tables to view various stored data with the DB browser

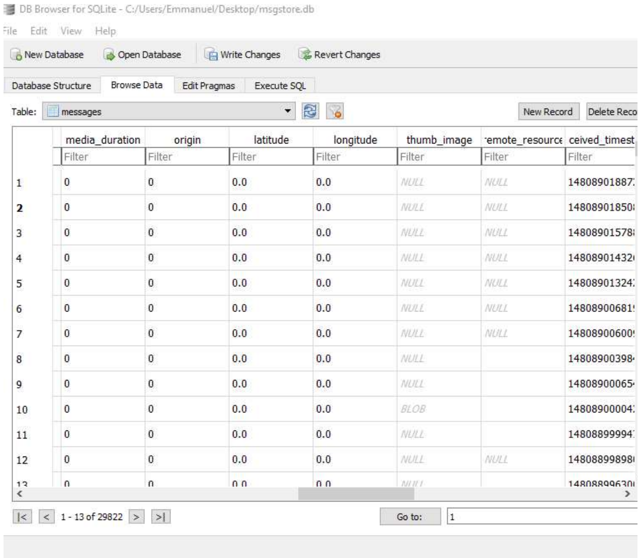
On selecting the appropriate table for exploration, a forensic investigator will see all the data stored and used by WhatsApp on that table. The message table contains all messages sent to and from contacts on the android device. The mobile number of message recipients and senders are stored under the field key_remote_jid in the format mobile-number@s.whatsapp.net while the messages are stored in the field data (Figure 12). The timestamp (unix format) media url (reference to images, video and audio files stored in the media folder of WhatsApp on the external memory card). Media name and cation fields also exist to store those data for media files for which they exist. The send and receive time stamp for each sent and received messages are also captured on the database. Although fields exist for storing the longitude and latitude of possible the device of the sender, none where recorded on the database table (Figure 13)


DB Browser for SQLite - C:/Users/Emmanuel/Desktop/msgstore.db

	key_remote_jid	_from_	key_ic	status	eds_pı	data
16619	2348035393552@s.whatsapp.net	0	56F...	13	0	Maybe network
16620	2348035393552@s.whatsapp.net	1	DA...	13	0	I don leave am message Sh
16621	2348035393552@s.whatsapp.net	0	91...	13	0	Okk
16622	2348035393552@s.whatsapp.net	0	A4...	13	0	No p
16623	2348035393552@s.whatsapp.net	1	63B...	13	0	Make em reply but I go buzz
16624	2348035393552@s.whatsapp.net	0	DE...	0	0	Aiit
16625	2348035393552@s.whatsapp.net	0	209...	0	0	Na Jst say u b fresher
16626	2348035393552@s.whatsapp.net	0	CC...	0	0	If nt
16627	2348035393552@s.whatsapp.net	0	D0...	0	0	No need call hm
16628	2348035393552@s.whatsapp.net	0	D4...	0	0	Jst pay hm must c and conf
16629	2348035393552@s.whatsapp.net	1	D8...	13	0	OhhOkay
16630	2348035393552@s.whatsapp.net	0	907...	0	0	Yea

16619 - 16630 of 29822

Figure 12: Contacts stored as remote keys and corresponding sent/received messages


DB Browser for SQLite - C:/Users/Emmanuel/Desktop/msgstore.db

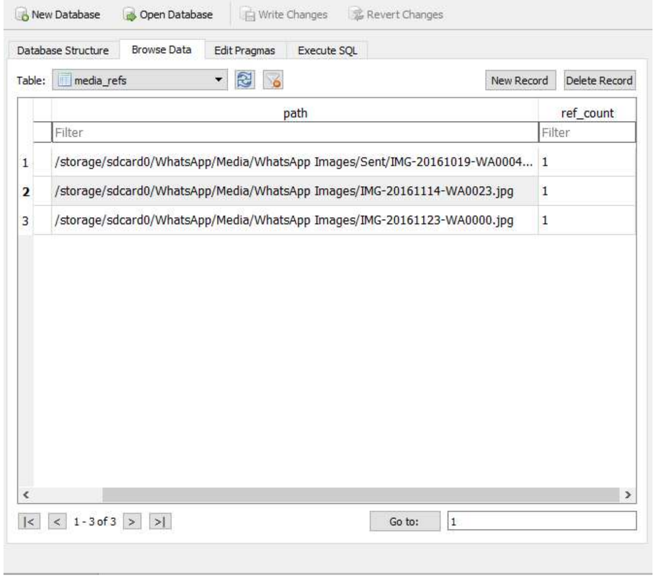
	media_duration	origin	latitude	longitude	thumb_image	emote_resource	ceived_timest
1	0	0	0.0	0.0	NULL	NULL	14808901887
2	0	0	0.0	0.0	NULL	NULL	14808901850
3	0	0	0.0	0.0	NULL	NULL	14808901578
4	0	0	0.0	0.0	NULL	NULL	14808901432
5	0	0	0.0	0.0	NULL	NULL	14808901324
6	0	0	0.0	0.0	NULL	NULL	14808900681
7	0	0	0.0	0.0	NULL	NULL	14808900600
8	0	0	0.0	0.0	NULL		14808900398
9	0	0	0.0	0.0	NULL		14808900065
10	0	0	0.0	0.0	BLOB		14808900004
11	0	0	0.0	0.0	NULL		14808899994
12	0	0	0.0	0.0	NULL	NULL	14808899898
13	0	0	0.0	0.0	NULL		14808899630

1 - 13 of 29822

Figure 13: Empty longitude and latitude fields

Although the longitude and latitude positions are currently not being captured, it is safe to infer that the developers are presently working on an update of the application that stores this details on the SQLite database which will be a vital information to forensic investigators as they will be able to determine the location of the device owner when messages are sent and received.

Although images are not stored on the database, it contains a table that stores the image paths as stored on the SD card (Figure 14).



	path	ref_count
1	/storage/sdcard0/WhatsApp/Media/WhatsApp Images/Sent/IMG-20161019-WA0004...	1
2	/storage/sdcard0/WhatsApp/Media/WhatsApp Images/IMG-20161114-WA0023.jpg	1
3	/storage/sdcard0/WhatsApp/Media/WhatsApp Images/IMG-20161123-WA0000.jpg	1

1 - 3 of 3

Figure 14: Media reference files stored on the media_refs table

The study was able to reach the same results as those of Gudipaty (2015) who decrypted a now legacy version of the encrypted database which uses a .crypt7 encryption key.

5. CONCLUSION

The methodology discussed in this study presents a forensically sound method of extracting data from a crypt12 encrypted database with a standard approach that can be applied to any forensic investigation that involves obtaining evidence from WhatsApp messenger on an Android smartphones. The procedure involves using a couple of open source tools to extract conversations from an android device under investigation which are encrypted with a crypt12 encryption at the time of this study and stored on the external memory card (SD Card) of the device if present or the internal memory of the android device if SD card is not present.

6. RECOMMENDATION

The major difficulty for any forensic investigation is the constant updating of the encryption standard used by WhatsApp application to protect the backups that are stored on the device from unauthorized read and write access. Earliest versions of the application stored backup copies of the database in a plain unencrypted manner making them easily readable and vulnerable for malicious users to exploit. The current version of WhatsApp uses crypt12 encryption keys which was formally crypt8. It is therefore very important for forensic investigators to keep themselves up to date about the current encryption of WhatsApp databases and available techniques that may be used to retrieve data from such database backups for the purpose of presenting forensic investigation.

REFERENCES

Abdulhamid, S. M., Abd Latiff, M. S., Chiroma, H., Osho, O., Abdul-Salaam, G, Abubakar, A. I. and Herawan T. (2017), "A Review on Mobile SMS Spam Filtering Techniques", IEEE Access, DOI: 10.1109/ACCESS.2017.2666785.

Abidin, N. Z. B. Z. (2015). Forensic Analysis Of Third Party Applications: Instagram. Forensic Focus.

Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. Digital Investigation, 9, S24-S33.

Anglano, C., Canonico, M., & Guazzone, M. (2016). Forensic analysis of the ChatSecure instant messaging application on android smartphones. Digital Investigation, 19, 44-59. doi: http://dx.doi.org/10.1016/j.diin.2016.10.001

Facebook to Acquire WhatsApp. (2014). [Press release]

Ibrahim, M. (2016). How to Decrypt WhatsApp crypt12 Database Messages. Retrieved October 30, 2016

Karpisek, F., Baggili, I., & Breitinger, F. (2015). WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages. Digital Investigation, 15, 110-118. doi: http://dx.doi.org/10.1016/j.diin.2015.09.002

Kim, E. (2015). "WhatsApp's Insane Growth Continues: 100 Million New Users in 4 Months". Business Insider.

Lohiya, R., John, P., & Pooja Shah (2015). Survey on Mobile Forensics. International Journal of Computer Applications, 118(16).

Mahajan, A., Dahiya, M. S., & Sanghvi, H. P. (2013). Forensic Analysis of Instant Messenger Applications on Android Devices. International Journal of Computer Applications, Volume 68– No.8.

Olsen, P. (2014). WhatsApp Hits 600 Million Active Users. Forbes.

Sahu, M. S. (2014). An Analysis of WhatsApp Forensics in Android Smartphones. International Journal of Engineering Research, Volume No.3(No.5), 349-350.

Statt, & Nick. (2016). "WhatsApp has grown to 1 billion users". Retrieved September 10, 2016

Thakur, N. S. (2013). Forensic Analysis of WhatsApp on Android Smartphones. (MSC in Computer Science, Information Assurance), University of New Orleans, University of New Orleans.

Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). Network and device forensic analysis of Android social-messaging applications. Digital Investigation, 14, Supplement 1, S77-S84. doi: http://dx.doi.org/10.1016/j.diin.2015.05.009

What Is an Android Phone? . Retrieved 02, December, 2016, from https://www.lifewire.com/definition-of-android-phone-578661

WhatApp. wikipedia. "Whatsapp Video Calling" (blog). Retrieved Dec 18, 2016.