Journal of
Information Technology & Software Engineering

Gudipaty and Jhala, J Inform Tech Softw Eng 2015, 5:2
DOI: 10.4172/2165-7866.1000147

Research Article Open Access

WhatsApp Forensics: Decryption of Encrypted WhatsApp Databases on Non Rooted Android Devices

Gudipaty LP* and Jhala KY

Digital Forensic Analyst eSF Labs Ltd, Hyderabad, India.

Abstract

The domination of social networking applications such as WhatsApp, Facebook, Viber continues to grow exponentially with WhatsApp being the undisputed leader amongst a vast series of social networking and chat messengers with more than 600 million users worldwide and being the number one paid application in more than 131 countries. However the easy availability and the affordability of a messaging medium like WhatsApp also makes its a top target for evil doers and criminals to misuse WhatsApp with malicious intents such as bullying, stalking, sharing threatening, abusive or pornographic content to victims. It is therefore very important to have a sound forensic methodology to extract potential evidences such as chat messages from devices running WhatsApp. The purpose of this research is to present 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 it into human readable formats.

Keywords: WhatsApp analysis; Android forensics; WhatsApp forensics; WhatsApp Crypt7; WhatsApp key file; Mobile forensics; BYOD forensics

Introduction

With the rapid evolution in the Smartphone technologies, the development industry has seen a sudden surge in the number of applications available for a Smartphone user. While there are many applications that cater to every one's needs, social networking applications occupy a lion's share in the number of users who frequently use them on a daily basis. Instant messengers available in the application markets are capable of transmitting a wide range of messages with no restrictions on message lengths and also allow you to share multimedia like videos, location, images, etc. All these services come at virtually no cost and one can avail this wide array of features for free simply by connecting the mobile device to the internet via data plans or WiFi connections. A research at Deloitte confirms the fact that an average person sends as many as 46 instant messages per day using such instant messenger applications and this industry is expected to be a transmission medium to a whopping 300 billion instant messages in this year. WhatsApp is one such application that is an undisputed leader amongst social networking and instant messenger applications. WhatsApp is cross-platform instant messenger service that has over 600 million users and continues to grow exponentially. It was recently acquired by Facebook which has made many new changes to the set of features that WhatsApp already provides. WhatsApp synchronizes with the phone book of the user and allows him to send such message to any contacts that have the same application installed on their device. It however may retain certain private information on the devices at specialized locations on the internal storage that a layman user may not be aware of. WhatsApp stores conversations of the user in database files as a backup in the internal storage or the SD Card of the mobile device. WhatsApp automatically makes backups every day at 4 AM and preserves in a folder named WhatsApp in the SD Card or internal storage of the Android Smartphone. The backups are maintained for a period of 7 days after which the oldest backup gets overwritten by the new backup. The chat backups are stored in a SQLite Format Database named msgstore.db in the sdcard/WhatsApp/Databases folder [1]. Earlier these databases were stored in a non-encrypted plain text format making it very easy for hackers to exploit the database files and extract chat conversations from them. Considering this a serious vulnerability, security experts at WhatsApp implemented a security mechanism by encrypting the stored backup files using a strong encryption algorithm to prevent or restrict unauthorized access. From a forensic investigation perspective, WhatsApp may contact volumes of evidentiary data that could be used in the court as evidence. Therefore it is highly crucial to have a methodology to be able to parse these encrypted databases in human readable format. This research paper propose a step by step process to acquire the encrypted backup files stored on the Android devices and decrypt them to obtain stored backup conversations from a suspect Android device and parse them in human readable format. The specialty of this approach is that it can be applied to both rooted and non-rooted Android devices. The backup conversations may contain valuable chat messages that may be deleted in existing messages. Extraction of such deleted messages is equally important from a perspective. This approach not only allows recovery of existing chats but may also help us retrieve deleted messages

Experimental Setup

A forensic workstation was set up in order to perform this experiment. It was configured with latest operating system and powerful hardware. The workstation was isolated from the network and installed with latest updated antivirus and anti-malware softwares to prevent evidence contamination or deletion due to virus attacks [2]. An unrooted Nexus 4 device (16 GB Model) Android version 5.0 (Lollipop) and running WhatsApp version 2.11.432 was used for the experiments

Tools and requirements

Software tools:

1) Android debugging bridge (adb.exe)

2) WhatsApp key/DB extractor (Version 2.2)

3) WhatsApp viewer (Version 1.6.0.0)

4) WhatsApp extract

***Corresponding author:** Gudipaty LP, Digital Forensic AnalysteSF Labs Ltd, Hyderabad, India, Tel: 9833532974; E-mail: laxmikant@esflabs.com

Received March 03, 2015; **Accepted** May 05, 2015; **Published** May 15, 2015

Citation: Gudipaty LP, Jhala KY (2015) WhatsApp Forensics: Decryption of Encrypted WhatsApp Databases on Non Rooted Android Devices. J Inform Tech Softw Eng 5: 147. doi:10.4172/2165-7866.1000147

5) Python (Version 2.7)

6) SQLite spy

7) Android backup extractor

Hardware:

1) Forensic workstation (Intel i5, 8GB DDR3 RAM, 1 TB Seagate HDD, Windows 8 OS)

2) USB data cable

3) LG Google Nexus 4

Methodology

The first step to perform acquisition of WhatsApp database file is connecting the mobile device to the forensic workstation using the corresponding data cable. On connecting successfully, the mobile device will display in My Computer as Portable Media Player (Figure 1). Browse to the folder named WhatsApp and then browse in a folder named Databases (Figures 2 and 3). Displayed below are the lists of encrypted database backups which are present on the Nexus Device (Figure 4). 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. On un-rooted devices, it is not possible to access this part of the mobile device; therefore we require an alternative solution to extract the key files present in the RAM. For this purpose, we use a tool called "Whats App Key/DB Extractor (Version 2.2)". This software also works for un rooted Android devices and successfully extracts the

Figure 1: Suspect device attached to forensic workstation.

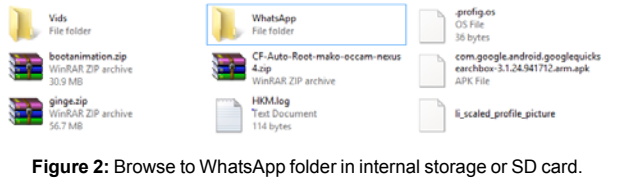

Figure 2: Browse to WhatsApp folder in internal storage or SD card.

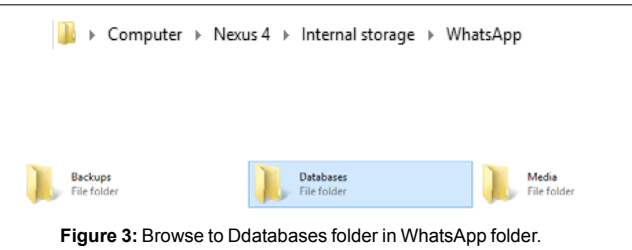

Figure 3: Browse to Ddatabases folder in WhatsApp folder.

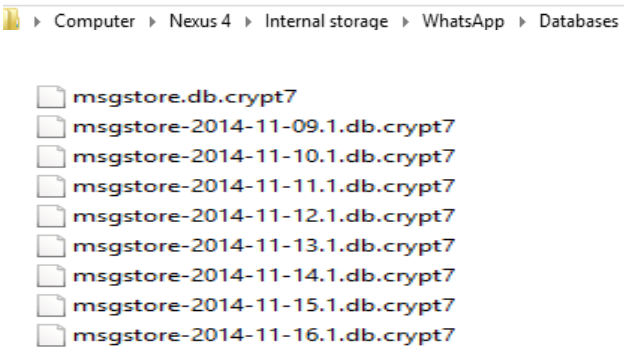

Figure 4: List of encrypted databases present in internal memory.

Figure 5: Enabling USB debugging on Android device.

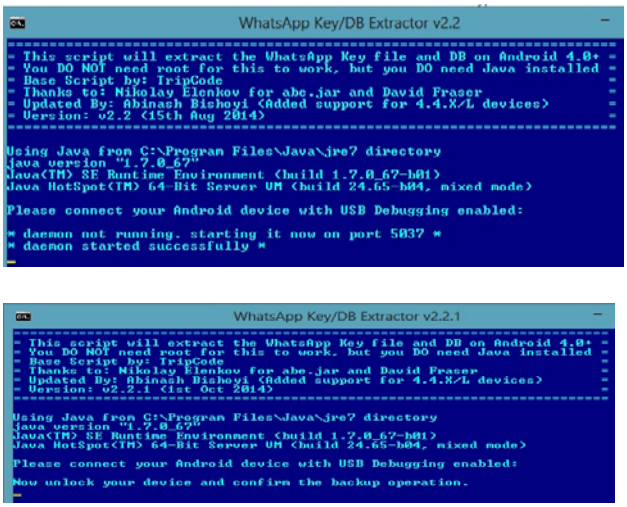

Figure 6: Executing WhatsApp Key/DB extractor.

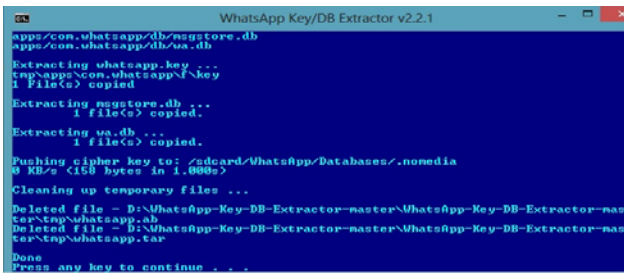

Figure 7: Extraction of key and dabatase file completed.

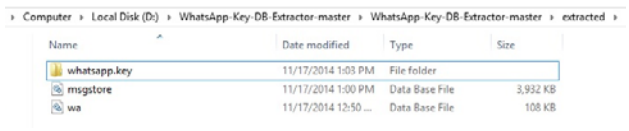

Figure 8: List of files extracted by WhatsApp Key/DB extractor.

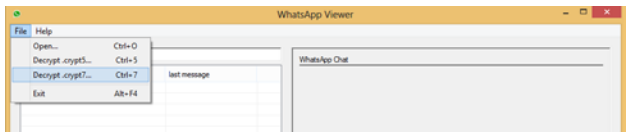

Figure 9: User interface of WhatsApp viewer.

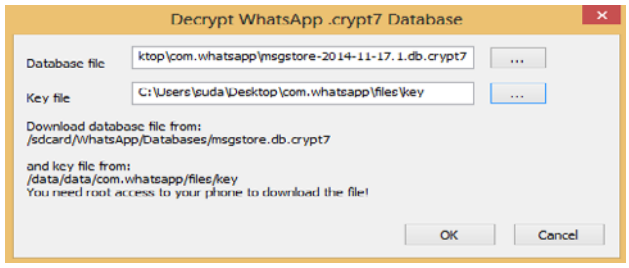

Figure 10: Provide the db.crypt database and extracted cipher key.

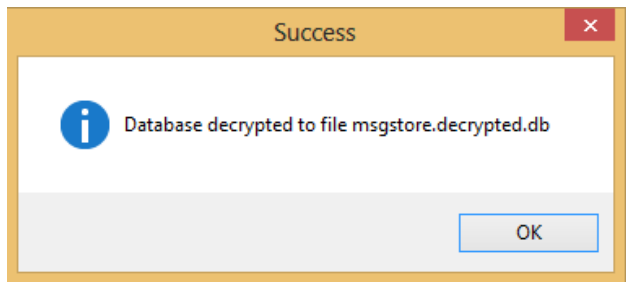

Figure 11: Successfully decrypted the encrypted database.

Figure 12: Decrypted database viewable in SQLite browser.

Figure 13: Open the decrypted database in SQLite SPY and view the chat messages.

existing msgstore. db file which contains the existing undeleted chats in decrypted format. It also carves out the key file which is needed to decrypt the encrypted backups which have been extracted from the internal as shown above [3].

The prerequisite step to run this tool is enabling USB debugging mode from the Settings Menu on the Mobile device. The steps require enabling this feature are:-

- Go to Settings
- Go to About Phone
- Tap Build Number 7 times

You will get a message saying "You are now a Developer"

- Click on Developer options in newly enables 'Developer Mode" (Figure 5).

Once this is enabled, execute the WhatsApp Key/ DB Extractor (Figures 6 and 7).

The files that are extracted are stored in a folder named 'extracted" in the same folder as the WhatsApp Key/DB Extractor (Figure 8). The msgstore.db is the database file containing the WhatsApp conversations whereas the wa.db contains a complete listing of a WhatsApp user's contacts including phone number, display name, timestamp, and any other information given upon registering with WhatsApp. In order to parse the output of msgstore.db, we need software named WhatsApp Extract which is a Python Script to interpret WhatsApp conversations and display them in human readable format[4]. However if we wish to decrypt the WhatsApp encrypted databases which we extracted earlier from the internal storage, we need to use a decrypter named WhatsApp Viewer and supply it with the crypt7 key file that we carved out using WhatsApp Key Extractor Supply the software with the msgstore. db.crypt file and the key file that we previously extracted. Ensure that you keep both the files in the same folder for clear output (Figures 9-11).

This will create a file named msgstore decrypted.db in the folder (Figure 12). This database file can now be opened directly in any of the available SQLite database parsers such as SQLite Manager, SQLite Spy or SQLite Database Browser. For our experiment we use a free software "SQLite SPY" (Figure 13) [5]. Thus we have successfully managed to parse the output of encrypted WhatsApp backup files by decrypting the backup databases using crypt7 cipher key file which was carved out of RAM of the mobile device. The above mentioned procedure can be used in cases where we wish to extract conversations from backups of an older date. It can be very useful in cases where some of the conversations have been deleted and do not exist in current databases. It may be possible that the conversation in question may exist in one of the backups that have been made on a previous date. The above mentioned procedure is not mandatory if we have the msgstore.db file which has been fetched by the WhatsApp DB/Key Extractor since it automatically extracts the unencrypted msgstore.db directly from the internal memory (RAM) that can directly be opening any SQLite browser or using a parser such as WhatsApp Extract

Challenges

While the above mentioned methodology is fairly straightforward to acquire backup conversations and messages from WhatsApp databases, it may be possible that a forensic investigator may encounter challenges while performing data recovery. Mentioned below is the list of challenges that a forensic examiner may face.

1) The device in question may be password protected or pattern protected

2) The application may be locked using any third party application locker tools

3) The device screen may be damaged or broken

All the above mentioned challenges will disallow enabling of the

very important feature of enabling "USB Debugging" which has been mentioned in the methodology. In absence of this feature, it would be impossible to extract the key file which is stored in the internal memory. Therefore, inspite of having the encrypted database files, it won't be possible to m decrypt them into plain text in the absence of a valid cipher key. Also, extraction of this key is only possible in devices running Android version higher than 4.0 since the Android backup option is only available in Android versions after 4.0 [6].

Conclusion

The methodology discussed in the research for extraction of WhatsApp's encrypted databases is a standard approach that can be applied to any forensic investigation that involves use of WhatsApp messenger in Android smartphones. It is fairly straightforward procedure to extract chat conversations in the WhatsApp backup location stored on sdcard or internal storage using a WhatsApp key extractor and a decryptor to convert the backup databases into plain text databases that can be viewed in any SQLite database browser. However the major challenge for any forensic examiner is the frequent updation of encrpytion standards that WhatsApp uses to protect these backups from unauthorized access. The earliest versions of WhatsApp would store these backup files in plain text making them easily readable and vulnerable for exploitation. Keeping user privacy and application security in mind, the encryptions used to protect these databases constantly get update and the current version of WhatsApp uses crypt7 encryption keys. It is therefore highly important for forensic investigators to keep themselves updated with the changes in technology pertaining WhatsApp backup databases in order to be able to extract snippets of chat conversations that may be present on suspect device.

Acknowledgment

This work was supported by eSF Labs Ltd, Hyderabad, India, that provided the technical conditions and the forensic workstations and lab setup used for the development and testing of the solution.

References

1. The SQLite Official Documentation
2. Hoog A (2011) Android Forensics - Investigation Analysis & Mobile Security for Google Android, Elsevier.
3. Quick D, Alzaabi M (2011) Forensics analysis of the Android File System YAFFS2, Austrailian Digital Forensics.
4. Cortjens M, Spruyt DA, Wieringa WFC(2011) WhatsApp Database Encryption Project R.
5. Creating Android Backups
6. Android Backup Extractor