International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print)
Volume No.3, Issue No.5, pp : 349-350 01 May 2014

An Analysis of WhatsApp Forensics in Android Smartphones

Mr. Shubham Sahu
Pursuing Bachelor of Engineering in Computer Science & Engineering | Founder – Chhattisgarh InfoSec Society (NGO)
cybersecurityguru@gmail.com

Abstract — WhatsApp is mobile application which allows exchange of messages, videos, audio's and images via Smartphone. The increased use of IM on Android phones has turned to be goldmine for mobile and computer forensic investigators. This paper focuses on conducting forensic data analysis by extracting useful information from WhatsApp and from similar applications installed on Android platform.

Keywords — WhatsApp, Android Forensics, WhatsApp Security, Data Security.

I. Introduction

Whatsapp allows to text messaging, send images, video, and audio media messages. The application is available for Android, Blackberry, iOS, Symbian (s60), and Windows phone. Whatsapp Inc. was founded in 2009 by Brian Acton and Jan Koum, both veterans of Yahoo!

People are exchanging information like images, videos, activities and events. But despite of getting connected with friends for more and more time, their privacy is also getting more vulnerable to threats by hackers and cyber criminals.

There is no restriction on the length and number of messages one can exchange and no carrier IM fees apply. One does not need to install a sim-card to use WhatsApp; the only requirements are a supported phone, internet connection and storage space on the phone to download the application.
WhatsApp uses a customized version of the open standard Extensible Messaging and Presence Protocol (XMPP). After WhatsApp is installed in any mobile, it creates a user account using the phone number as the username (ID: [phone number]@s.whatsapp.net). WhatsApp automatically synchronizes all the phone numbers from user's phonebook with its centralized database of WhatsApp users to add contacts to the user's WhatsApp contact list.
Previously, WhatsApp messages were not encrypted, that means data which was sent and received was in plaintext, meaning messages could easily be read easily if packet traces were available.

WhatsApp NOW AND BEFORE
WhatsApp data is stored in the Internal Memory of the mobile phone. After it is installed, it automatically synchronizes with the phone's contacts showing users who are already using WhatsApp.
When a mobile with WhatsApp installed is turned on, "*com.whatsapp*" process receives a signal to start the '*ExternalMediaManage*' and '*MessageService*' services which runs in the phone's background till the phone is turned on.
Before
With the starting version of WhatsApp 2.9 the messages exchanged was stored in 'msgstore.db' which is SQLite databases. But in early versions security researchers found that the chat records which was handled by WhatsApp was vulnerable, because the database file which saves the chat conversations was not encrypted and can easily accessible through many ways to get the whole conversation chat details including images, videos, contacts and so on. As this news hits the internet, security researchers started researching with WhatsApp database (msgstore.db) to retrieve the conversation even the deleted ones from the chat option. But WhatsApp reacted soon and came up with an encryption mechanism to protect its database.

Now
Now, according to officials of WhatsApp they are taking the conversation database security in a very serious manner, now WhatsApp database encryption having custom AES encryption algorithm with above 192-bit encryption key mainly used for WhatsApp Android Platform. So now the previous file *msgstore.db* is converted to *msgstore.db.crypt*.

II. Material and Methodology

The major problem after having the file *msgstore.db.crypt* is its decryption. Thanks to contribution of Francesco Picasso who made a tool to decrypt and organize SQLite database files in an organized HTML form. The tool works for both encrypted and decrypted database files. The WhatsApp Database Encryption Project has made known a vulnerability in the Android implementation of the AES Cipher: the 192-bit key can be detected performing both static or active analysis on the software package.
A python script uses this same key to decrypt the encrypted db file and presents the result in a well organised HTML page. The paper implies that the same encryption key is used for all WhatsApp installations on Android. In this methodology, we have used this Python tool to decrypt and read our encrypted database and it was done successfully with the latest version of WhatsApp 2.11.186. We can alternately read the database files through the 'SQLite browser' but the timestamps and representation of data is not straightforward. Another advantage of WhatsApp Xtract tool is that all the media contents that are exchanged are displayed on the HTML page itself, one does not have to look into the media folder separately. The tool can be useful in comparing the data we analyze.

Finding the information:
WhatsApp stores all its chats on a SQLite database: The path of database file is different from platform to platform.

Android:
(/sdcard/WhatsApp/Databases/msgstore.db.crypt)

iOS:

ISSN:2319-6890)(online),2347-5013(print)
01 May 2014

(Application/net.whatsapp.WhatsApp/Documents/ChatStorage.sqlite)

Main Features:

- WhatsApp database can be inspected for both iOS (ChatStorage.sqlite) and Android (msgstore.db & wa.db) devices;
- Emoticons and attachments (images / video / audio / gps / contacts) are shown in the message content.

How to use:

Step 1:Download WhatsApp Xtract package on your computer and extract it.

Step 2: Download and install Python programming language environment on your computer.

Step 3: Open the folder where you downloaded the WhatsApp Xtract archive. Find a file with name *!install pyCrypto.bat*, right click on it and click run as administrator. This bat file will execute the following Python command, *pypm install pycrypto*. This common automatically installs the pycrypto library on your computer, which will be used to decrypt the WhatsApp backup data.

Step 4: In the same folder, run either
whatsapp_xtract_iphone.bat,
whatsapp_xtract_android_crypted.bat *or*
whatsapp_xtract_android.bat
Depending upon the backup file you used. To run any of these files, simply right click on it and click run as administrator, just like above.
You can also run *whatsapp_xtract_console.bat* to specify the WhatsApp backup file manually.

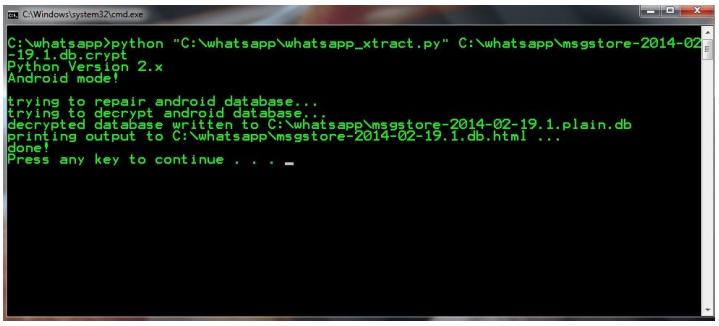
/* For Android DB: */
python whatsapp_xtract.py -i msgstore.db -w wa.db

/* If wa.db is unavailable */
python whatsapp_xtract.py -i msgstore.db

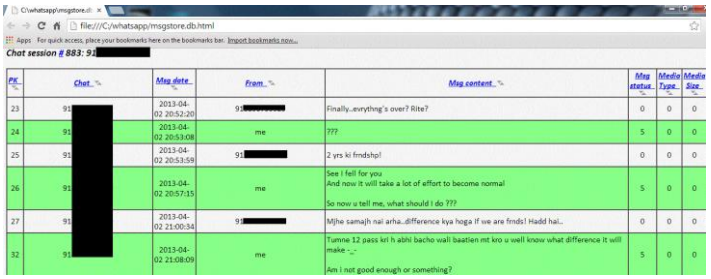
/*For crypted DB*/
python whatsapp_xtract.py -i msgstore.db.crypt

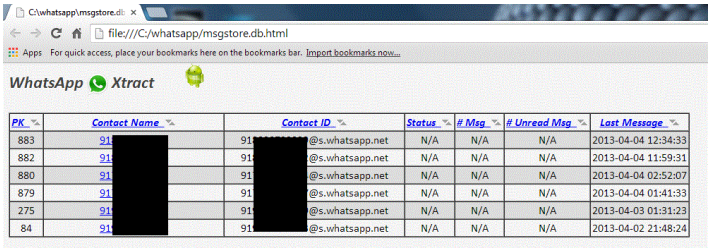
/*For iPhone DB*/
python whatsapp_xtract.py -i ChatStorage.sqlite

Results



As soon as the execution of the bat file or command is completed, all your WhatsApp backup data will be decrypted and will be displayed in the default browser on your computer.





IV. Conclusion

When doing a forensic investigation, having the most recent messages for analysis can play a vital role. In addition to the recent messages one can look into deleted messages as well. Thus, retrieving the artefacts after the factory reset of the phone or retrieving the deleted data can be taken as the future aspect.

Acknowledgement

I would sincerely like to thank Reader(s) of Department of Computer Science, REC Raipur - Prof. Anurag Sharma & Prof. Uzma Ansari for their excellent guidance and support. Their exceptional knowledge, wisdom and understanding have inspired and motivated me. I would also like to thank Mr. Saket Modi, CEO of Lucideus Tech Pvt Ltd for his guidance.

References

i. http://en.wikipedia.org/wiki/WhatsApp
ii. https://play.google.com/store/apps/details?id=com.whatsapp
iii. "Forensic Analysis of Instant Messenger Applications on Android Devices." : *IJCA 2013.*
iv. Zena Forensics "WhatsAppXtract" Tool - (Available Online) http://code.google.com/p/hotoloti/downloads/list
v. http://developer.android.com/guide/components/fundamentals.html
vi. "Android Forensics, 1st Edition" *: Andrew Hoog*
vii. "WhatsApp Database Encryption Project Report" : *Cortjens, D., A. Spruyt, and W. F. C. Wieringa.*
viii. Whatsapp Hacking 2013 : *Lucideus Tech Pvt. Ltd.*
ix. Forensic Analysis of WhatsApp on Android Smartphones : *University Of New Orleans.*
x. Open source tools for mobile forensics: *Sans European Digital Forensics Summit.*