Acquisition and Analysis of Artifacts from Instant Messenger on Android Device

Mathavan T
Department of Information Technology,
SRM University, Kattankulathur, Chennai, India

Nagoor Meeran A. R
Department of Information Technology,
SRM University, Kattankulathur, Chennai, India

***Abstract* — The modern day Smartphone's have built in apps like "WhatsApp" which allow users to interchange instant messages, share videos, audio's and pictures through Smartphone's instead of depend on their desktop Computers or laptop thereby increasing the portability and convenience for a layman smart phone user. An Instant Messenger (IM) can serve as a very valuable yet very daring platform for the prey and the suspicious to communicate. The larger use of Instant messengers on Android phones has turned to be the treasure house for mobile and computer forensic experts. Traces and Evidence left by applications can be held on Android phones and recovering those prospective evidences with right forensic method is strongly essential. This paper focuses on conducting forensic data analysis of one of the widely used IMs applications on Android phones: WhatsApp. An Android phone was investigated tests and analysis were performed with the aim of determining what data and information can be found on the device's internal memory for instant messengers e.g. message logs and history, send & received image or video files, etc. Determining the location of data found from File System Extraction of the device was also determined. The analysis and results show that heavy amount of potential evidences and valuable data can be found on Android phones by forensic investigators.**

General Terms

Android, WhatsApp, Mobile Forensics, Application Security, Information Assurance, Data Security, Computer Science, Volatile Memory.

I. INTRODUCTION

There has been speedy growth in online communication in the past 7-8 years, particularly in mobile communication. Smartphone's have taken up the market so well that everybody now can interact, socialize, and can share ideas and Information sitting at any corner in the world. Today's new generation is busy in chitchat and messaging every time with friends and with unknowns too. People are continuously 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 susceptible to threats by hackers and fraudsters. This is because criminals know that doing crimes using online mobile applications is secure as it is very hard-hitting task for extracting the information from mobile phone from which crime was committed. This is so because mobile phones have very less memory and that too they have flash memory which gets washed fast and easily on mobile phones. One more Reason of using mobile applications for doing any crime is that their application logs will not get saved at Internet Service provider side. Whatsapp is the most widely used instant messaging application with more than 100000000 + downloads (On Google Play).

II FORENSIC CHALLENGES AND STORAGE ARTIFACTS

In any forensic investigation of the Android phones, a forensically sound approach has to be taken care at the most. The equipment's, background and methods to be used should be as per the prime rules of computer forensics. A forensically sound policy neither changes any data on the original device nor will it write any data on it. This paper focuses on the forensic analysis of the data stored by Whatsapp. But prior to examination of data, it is needed first to discover & extract the files and folders where the artifacts related to the applications have been stored in the internal memory of the phone. But forensic investigation of applications and their databases is tough if it's encrypted or deleted. Also, Android phone users are mostly connected to Internet every time, so data can be wiped remotely by any person. Also, Updates are incessantly out by the developer of the application and Operating system installed in the phone which makes it hard for forensic examiners to understand every updated feature and to be ready to deal with new methods of forensic examination with available old tools only. Also, update creates more Challenges for Law Enforcers and forensic investigators to prove and provide the evidence in court of law.Table-1 shows the features that are available in WhatsApp.

Table-1.Whatsapp features

Applications	**Features**
Whatsapp	1. Text Chat 2. Send & Receive Images 3. Send & Receive Videos 4. Send & Receive Audio's 5. Group Chat 6. Sharing V-Cards & Contact Information

III.PROPOSED METHOD

Thumb rule in any forensic investigation is not altering the evidence media. For proceeding the investigation further the examiner needs to take an image of the evidence media. Usually the forensic investigators will use equipment's like CelleBrite UFED for taking the image of the evidence media. Equipment will cost around some lakhs of money. To reduce the amount of money spend on purchasing the equipment. Through my research we developed a tool with that tool we are going to prove that the image taken from the evidence media is not tampered and also we are going to analyze the artifacts that are left by the instant messaging application WhatsApp. The method for acquiring the data is a bit tricky. However an updated version of dd maintained by the Department of Defense's Cyber Crime Center is used for the data acquisition. The program, DC3DD [9], is a patched version of GNU dd and includes a number of features useful for computer forensics. A shell script is written with DC3DD [9] for acquiring the bit by bit copy of the evidence media. Write protected cable is used for connecting the evidence media to the workstation in order to maintain the integrity. Before connecting the evidence media to the workstation the USB debugging mode in the android mobile phone needs to be enabled. For analyzing purpose we are going to use some commercial tools available in the market like winhex, HxD. Proving the integrity of the acquired mage by calculating the hash value before and after taking the image of the android mobile phone. Table-2 shows the list of hardware's and software's used in this research.

Table-2 List of hardware's and software's used for research.

List of Hardware's and Software's	**Versions**
Android phone - SONY WT19i	Ice Cream Sandwich-4.0.4
WINHEX	17.3
Whatsapp	2.11.186
Ubuntu	13.04
Android adt-bundle-Linux	X86
WhatsApp Xtract	2.1
SQlite Browser	2.0

3.1. Data acquisition and analysis from SD Card.

WhatsApp stores its user data in a SQLite database (msgstore.db and wa.db). The location and structure of the database varies from platform to platform. Here we are engaged on devices with the Android platform. If one picks not to root the device one can gain access to the backed up WhatsApp folder on the SD card. This folder mainly comprises three sub-folders such as:

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

The file is encrypted and present on the SD card at:

/sdcard/WhatsApp/Databases/msgstore.db.crypt

The WhatsApp Database Encryption Project [4], implies that the similar AES with a 192-bit encryption key is being used for all WhatsApp installations on the Android platform.
346a23652a46392b4d73257c67317e352e3372482177652c

WhatsApp Xtract [3] has presented a basic Python script that takes an encrypted db file (msgstore.db.crypt) as input and gives a decrypted db file (msgstore.plain.db) as output. The output file can be read using the SQLite browser software.

We used an open source tool – WhatsApp Xtract [3], in order to be able to read the information in a more human understandable form and match our results in the SQLite browser. With this tool one can open the media files and see the messages straight from the output HTML file.
Further one can also advance admission to other sub-folders in the WhatsApp folder on the SD card like:

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

The data in these folders is not encrypted. The Media folder covers all the media files such as Audios, Videos and Images swapped during a chat session with the current user. Backup of the files from the device to the SD card is made every day around 4:00 a.m. Absence of the most recent data from the decrypted database or the media folder only means that the application has not backed up the up-to-date data into the database on the SD card for today yet.

On the other hand if one roots the device we see that the plain database files wa.db and msgstore.db, which can be found directly on the SD card at:
/data/data/com.whatsapp/databases/ msgstore.db and wa.db

On gaining root access to a device almost all of the application data stored on the internal storage turn out to be unrestricted. One can get forensic evidence from the phone whether the device under analysis is rooted or not. We are going to prove the integrity of the image by generating hash value before and after taking the image from the android mobile phone. The hashing algorithm used is SHA256 Table-3 shows the generated hash value.

Table-3 Hash value generated from android mobile before and after creating the image.

Sony WT19i	**Hash Value**
Before taking the image	B175DAD11A1BDDD55 BB186F2A4D720A3F989 BCC2475F3C2D5EAF86F 45E90A107
After taking the image	B175DAD11A1BDDD55 BB186F2A4D720A3F989 BCC2475F3C2D5EAF86F 45E90A107

3.2. Data Acquisition and Analysis - Internal Memory.

The internal memory contains important information for any investigator as it has the most recent information accessed through the phone. A mobile has turn out to be the salvation of most humans and an IM application (like Whatsapp) on it says a lot about what a person has been doing currently. We need to get a grip of all that information now we will see how that information can be collected and analyzed in time. With the help of the same DC3DD [9] command we are taking the image of the internal memory. Through our research we found that the needed artifacts are not found in the internal memory.

IV.CONCLUSION

WhatsApp has become a popular application for social networking on which people may be exchanging their personal and business associated information. Our study has shown that one can get complete access to all that information in WhatsApp. The technique we took gave a wide-ranging summary for all related applications that run on Android devices. We were able to productively complete the aim of our study. Table -3 proves the integrity of the image acquired by our tool. Table -4 shows the artifacts found during the research. One should be aware that a password-locked phone is not a black box and one can extract valuable application user information from the database and volatile memory. Our future work will concentrate on how to extract the data from the RAM memory.

Table-4 Artifacts Found

	Non-Volatile Memory (SD Card) + No Rooting device	Non-Volatile Memory (SD Card) + Rooting Device
msgstore.db	Found Encrypted	Found Decrypted
wa.db	Not Found	Found
Phone Numbers	Found if DB Decrypted	Found
Messages	Found if DB Decrypted	Found
Media Files	Found if DB decrypted	Found
Contact Cards	Found if DB decrypted	Found
Profile Pictures	Not Found	Found

ACKNOWLEDGMENT

Am grateful to the principal and management of SRM University for extending all the facilities and constant encouragement for carrying out this research work. Also heartily thank Mr.A.R.Nagoor Meeran for giving me an opportunity to complete this research. You have been a tremendous mentor for me. I would like to thank you for encouraging my research. Your advice on both research as well as on my career have been priceless.

REFERENCES

[1] http://en.wikipedia.org/wiki/WhatsApp
[2] https://play.google.com/store/apps/details?id=com.whatsapp
[3] Zena Forensics "WhatsAppXtract 2012" [Online]. Available: http://code.google.com/p/hotoloti/downloads/list http://blog.digital-forensics.it/2012/05/whatsapp-forensics.html
[4] Cortjens, D., A. Spruyt, and W. F. C. Wieringa. "WhatsApp Database Encryption Project Report."
[5] "Android Forensics Investigation, Analysis, and Mobile Security for Google Android" by Andrew Hoog
[6] Mohammad Iftekhar Husain, Ramalingam Sridhar (2010) iForensics: Forensic Analysis of Instant Messaging on Smart Phones http://link.springer.com/chapter/10.1007%2F978-3-642-115349n_2?LI=true#
[7] Kailash Kumar, Sanjeev Sofat, S.K.Jain, Naveen Aggarwal (2012). Significance of Hash Value Generation in Digital Forensic: A Case Study. International Journal of Engineering Research and Development. Available at: http://www.ijerd.com/paper/vol2-issue5/I02056470.pdf.
[8] Curran, K., Robinson, A., Peacocke, S., Cassidy, S.(2010) Mobile Phone Forensic Analysis, International Journal of Digital Crime and Forensics, Vol. 2, No. 2, pp:, April-May 2010, ISSN: 1941-6210, IGI Pub
[9] About DC3DD: http://itandforensics.anima-web.us/2011/12/dc3dd-and-ddrescue.html
[10] Andre Morum de L. Simao, Fabio Caus Sicoli, Laerte Peotta de Melo, (2011) ACQUISITION OF DIGITAL EVIDENCE IN ANDROID SMARTPHONE. http://igneous.scis.ecu.edu.au/proceedings/2011/adf/9thADFProceedings.pdf#page=122