UNIVERSITI PUTRA MALAYSIA

A FORENSICS ACQUISITION METHOD OF WHATSAPP DATA ON ANDROID SMARTPHONE

UMMU KHOSYATILLAH BINTI MUZAKIR

FSKTM 2018 48

A FORENSICS ACQUISITION METHOD OF WHATSAPP DATA ON ANDROID SMARTPHONE

By

UMMU KHOSYATILLAH BINTI MUZAKIR

Thesis submitted to the Faculty of Computer Science and Information Technology, University Putra Malaysia, in fulfillment of the requirements for the Master of Information Security

JUNE 2018

COPYRIGHT PAGE

DEDICATIONS

"This sweet dedication goes to respected lecturers, thoughtful friends and supportive family"

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Information Security

A FORENSICS ACQUISITION METHOD OF WHATSAPP DATA ON ANDROID SMARTPHONE

By

UMMU KHOSYATILLAH BINTI MUZAKIR

JUNE 2018

Supervisor: Dr. Mohd Taufik bin Abdullah
Faculty: Faculty of Computer Science and Information Technology

Technology evolution in mobile devices and smartphones are kept progressing in demand. The environment of mobile devices is defined as personal usage; isolating the security priority at very beginning. Prior to the reason, it becomes a daring new target for the cybercrimes. WhatsApp application known as most widely used for communication platform, as well as a bold aim to perform mischiefs. Thus in this thesis, we propose the forensically sound method of data acquisition and analysis of WhatsApp application on Android smartphone. We will form guidelines on how forensic investigators extract the artifacts from WhatsApp. By having the artifacts, forensic investigators enable to describe on how the artifacts can be generated, describe relationship of the artifacts and the analysis can be done. The results gained by the method proposed in this thesis are at par with popular mobile forensic tools such as Cellebrite.

Keyword: Android Forensics, data acquisition, Mobile Forensics, WhatsApp.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia Sebagai memenuhi keperluan untuk Ijazah Sarjana Keselamatan Maklumat

A FORENSICS ACQUISITION METHOD OF WHATSAPP DATA ON ANDROID SMARTPHONE

Oleh

UMMU KHOSYATILLAH BINTI MUZAKIR

JUNE 2018

Penyelia: Dr. Mohd Taufik Abdullah
Fakulti: Fakulti Sains Komputer dan Teknologi Maklumat

Evolusi teknologi telefon pintar semakin berkembang seiring dengan wujudnya permintaan daripada para pengguna. Pada peringkat permulaan, teknologi ini merujuk kepada penggunaan peribadi berbanding keutamaannya dalam skop keselamatan. Justeru, kelemahan itu menjadi sasaran utama untuk penjenayah siber. Aplikasi WhatsApp merupakan salah satu aplikasi pesanan ringkas yang popular, dalam masa yang sama menjadi bidikan yang sesuai untuk melakukan jenayah ini. Oleh itu, kami bincangkan prosedur pengambil alihan data dan analisis yang dikendalikan untuk persekitaran aplikasi WhatsApp. Selain itu, kami menyediakan garis panduan mengenai bagaimana penyiasat forensik mengeluarkan artifak dari WhatsApp. Para penyiasat forensik mampu memperjelaskan bagaimana artifak dikenalpasti, mengaitkan hubungan antara artifak dan analisis yang dihasilkan. Hasil yang diperolehi dengan kaedah yang dicadangkan setanding dengan alat forensik yang popular seperti Cellebrite.

Kata kunci: Android Forensics, pengambil alihan data, Mobile Forensics, WhatsApp

ACKNOWLEDGEMENT

Alhamdulillah, all praises to Allah. Allah does not wish to impose hardship upon you rather He wishes to purify you. Allah promised us in the Holy Quran "And your Lord says: "Call on Me: I will answer your (Prayer): but those who are too arrogant to serve Me will surely find themselves in Hell- in humiliation!" (Al Mukminun: 60). Pray, because Allah always listen. Thank you Allah for the love, opportunity and guidance.

First and foremost, I would like to dedicate this gratitude to my lovely parents, Encik Muzakir bin Musjamil and Puan Faridah binti Alang Kamarudin. No matter how badly I failed, I always knew that you would treat me like a winner. Thanks for being supportive. Next my appreciation goes to my great supervisor, Dr. Mohd Taufik Abdullah who dedicated in give the constructive criticism. I am very thankful towards his effort, knowledge and infinite support. All the thorns placed in my path and the pain forced me to the new routes which ultimately to the success of this project.

Not to be forgotten, thanks to all my beloved teachers, lecturers, my precious family members, my teammates, my fellow friends and my dear students who are always lending their helping hands and understanding. May Allah shower all of you with His blessings. For those who still in the struggle: Give yourself a pat for making it this far. May Allah ease!

APPROVAL FORM

This thesis was submitted to the Senate of University Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master Information Security. The members of the Supervisory Committee were as follows:

DR. MOHD TAUFIK ABDULLAH

Faculty of Computer Science and Information Technology

University Putra Malaysia

(Supervisor)

Date: June 2018

DECLARATION FORM

Declaration by graduate student

I hereby confirm that:

- This thesis is my original work
- Quotations, illustrations and citations have been duly referenced
- This thesis has not been submitted previously or concurrently for any other degree at any other institutions
- Intellectual property from the thesis and copyright of thesis are fully-owned by University Putra Malaysia (UPM)
- Written permission must be obtained from supervisor and Deputy Vice-Chancellor (Research and Innovation) before thesis is published in book form
- There is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity was upheld as according to Rule 59 in Rules 2003 (Revision 2013-2014). The thesis has undergone plagiarism detection software

Signature: _____ Date: _____

Name and Matric No.: UMMU KHOSYATILLAH BINTI MUZAKIR (GS 47666)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

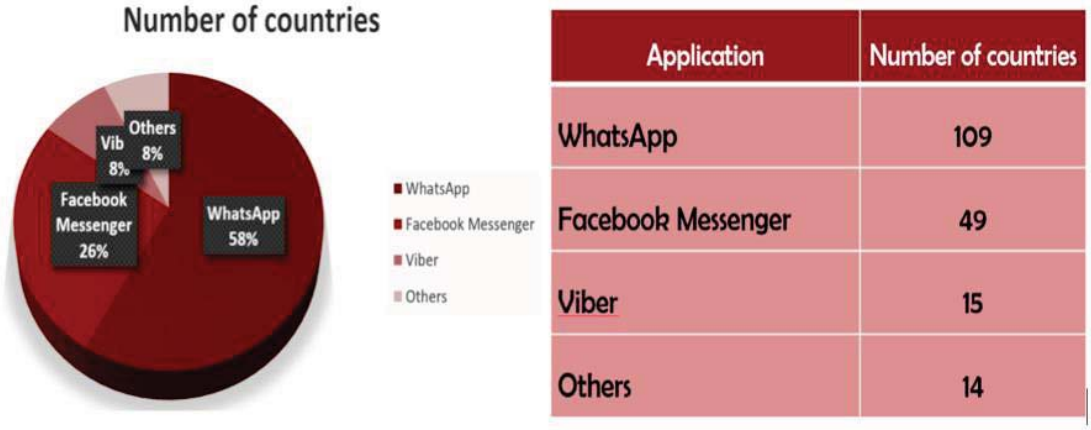
INTRODUCTION

1.0 Introduction

This chapter will briefly explaining introduction of background study of the related subject towards this project. Also, this chapter also consists problem statement, research objective, research scope, research result expectation and thesis structure. Research objective are derived from problem statement and expected to be achieved at the end of this project. Research scope and research schedule is to highlight the scope of this project and to ensure this project is on the right track according to schedule stated.

1.1 Background Research

Instant messaging, especially WhatsApp application is increasingly gaining popularity by leading as the most popular messaging app by 109 over 187 countries worldwide or 58% of the world as shown in Figure 1 (Indo-Asian News Service, 2016). Moreover, based on a study done by Venture Beat in 2017, Android wins the majority of 73% as the most widely used platforms within the WhatsApp users. On May 2018, the statistics conducted by Business of Apps analyzed the monthly active usage of this application and claimed its growth as the most vastly over another five; Facebook, Google, Gmail, Twitter and Skype.



Application	Number of countries
WhatsApp	109
Facebook Messenger	49
Viber	15
Others	14

Figure 1: The statistics of most used application regards number of countries and the application. (Indo-Asian News Service, 2016).

Mahajan et al. (2013) claims that due to its features of comprehensiveness and user-friendly, it is capable to lure the hackers, scammers and fraudst ers to the crimes using mobile applications. This statement is supported by Anglano (2014), Mathavan & Meeran (2014) and Shortall & Azhar (2015), which mentioned that WhatsApp could be used by organized crime groups to structure their illegal activities. According to Federal Investigation Agency, National Response Centre for Cybercrime, illegal activities such as blackmailing, transaction frauds and identity theft; as somebody's identity is stolen every 3 seconds are identified and reported as a result of cybercrimes done by this service.

Thus, since 2016 WhatsApp is established with the secure end-to-end encryption approach which disallow any issue of network being intercepted and ensures the communication between the sender and receiver is protected, not even to WhatsApp. Facebook, the owner of WhatsApp have a strong view that this action facilitates the data breach problem (Kanter, 2018). However, this activity makes it challenging to the investigators or law enforcement agencies when it comes to the case related to WhatsApp

messaging as it allows the difficulties in data interpreting and critical analysis to be done. This statement is supported by Adam and Shortall (2015), which stated that the encryption techniques used by such applications made traces of illegal activities almost undetectable.

Conger (2016) reported that WhatsApp has been blocked in Brazil four times within 12 months. One of the blockade is requested in May 2015 which involved the case of drugs and the WhatsApp's owner, Facebook failed to cooperate in hand over information that would be used and supported a criminal investigation. Due to end-to- end encryption policy, Facebook itself cannot access users' messages and unable to provide as per requested.

Also, by the reason of encrypted communication enforced by this application, the Telegraph reported that WhatsApp accused of giving terrorists 'a secret place to hide' as it refuses to share London's attacker's messages. The news mentioned that the attackers made WhatsApp as their medium of information exchanged. The authority failed to intercept the communication and almost missed the target criminals (Rayner, 2017).

Android platform allows an open development of an application, it is running at a very fast pace in terms of progress and it suits to the goal states "to accelerate innovation in mobile and offer consumers a richer, less expensive and better experience". However, as compared to iOS and Windows mobile OS, Android is more likely as a subject of targeting by the hacker. The statistic indicates up to October 2017, 69% of all devices infected over the past year ran a version of Android as their operating system (Walker, 2017). There are a great number of programs designed for the Android operating system, which data could be potentially be interesting to the investigator but there is no forensics program supporting analysis of logs and data from all of such programs (Mikhaylov, 2014).

Nevertheless, to keep data salvation, some skills are required such as the knowledge about programming, command line or network. This is important as to understand the clear view of developing an algorithm or suitable method. Also, the structure of databases which hold potential and relevant information must be studied. Apart from that, the most concern issues raised are the completeness evidence obtained and reliability of evidence to prove the crimes. Digital evidence has been an important component of the evidence presented in numerous high profile cases, but most often in litigation and prosecution cases of financial and criminal activities, accused personnel may deny or may not available for investigation as raised by Lone et. al. (2015). The current techniques used are known as preoccupied with the demands of the 'Daubert' principles, which is must consider these four criteria (O' Connor, 2004);

1. Has the theory or technique been reliable tested?
2. Has the theory or technique been subject to peer review?
3. What are the theories or techniques known or potential error rates?
4. Has theory or technique been generally accepted as a standard in its scientific community?

To maintain a good reputation and credibility of the investigators, the performance of managing security risk must be taken as consideration. The assets like information gained must be protected from any disclosure and modification. Hence, the practice of comprehensive method and understandable result during analysis stage is highly recommended.

1.2 Problem Statement

The forensic analysis regarding mobile devices is quite recent and there is no absolute technique recognized in this matter. Several works for WhatsApp Messenger forensics in Android field done by the researchers, but most of these works are limited in scope.

Command line such as dd and netcat sounds as powerful tool for artifacts acquisition. Thakur (2013) proposed this method but the scope is limited to SD card. However, Akbar and Krisnadi (2017) stressed that this technique only holds backup data. The backup process is a daily automated at 2.00 am and it depends to the activities done on that particular day which backup database file is totally different to system database file. Gudipathy and Jhala (2015) also mentioned that the data backup of SD card is preserved and maintained for seven days as the oldest backup gets overwritten by the new backup.

Thakur (2013) and Mahajan et al. (2013) focus on artifacts acquisition without emphasis on the critical analysis that should be conducted by relating the evidence. Without declaration on the acquisition method, Anglano (2014) broaden the scope by find the correlation points of the evidence and create the conclusion based on inference made.

In order to solve the problem mention above, a new acquisition technique for WhatsApp is proposed. The proposed method will allow a live environment of acquisition which has more sense on the changes of message exchanged; and also enable to have a comprehensive analysis by create the hypothesis.

1.3 Research Objective

The objective of this project is to propose an acquisition method for obtaining data of WhatsApp forensically from Android platform mobile devices. This method is enable do as follow:

1. To create a forensic bit-by-bit image of useful artifacts, and
2. To perform an analysis of useful artifacts in forensic image.

1.4 Research Scope

The scope of this project definitely focus on WhatsApp Messenger application and we recommend to practice in the version 2.17.** which it requires Android OS 2.3.3 or above. We required Linux Ubuntu and Windows 10 as platforms for this subject. As to find the relevancy of the technique suggested, we done some background studies in WhatsApp Messenger, Linux Ubuntu command and structure of Android and finally we decided to focus in memory acquisition. Also as to validate the relevancy of created image, we conduct some analysis as to compare and prove the propose method.

1.5 Research Schedule

This project is one year period which start in June 2017 and expected to finish in June 2018. Generally this project has six activities which are project implementation plan, knowledge gathering, experimentation design, implementation and development, testing and evaluation and lastly report write up. Each project activities have their own milestones

that need to be achieved. The details for project activities and time take can be refer in Gantt chart in Appendix section.

1.6 Thesis Structure

This chapter has provided a general overview of the entire thesis. The rest of the thesis is organized as follow:

Chapter 2: Literature Review. This chapter reviews related work on acquisition method for extracting useful artifacts and analysis of WhatsApp application on Android smartphone. This chapter also discuss issues and impact of mobile technology, acquisition method for extracting useful artifacts, technique to bypass mobile authentication and analysis techniques.

Chapter 3: Research Methodology. This chapter explains methodology that being used to develop this study. Methodology is one of essential element in every study as it to ensure the study is properly plan and can be execute smoothly. In this chapter also explained the framework that being used in this study.

Chapter 4: Implementation. In this chapter, the approach used to implement the proposed method is being explained in detail. Besides, the design and the functionalities of the approach also are highlighted. This chapter provides overall and process flow chart for this study. All the detail according to the implementation of the approach also can be found in this chapter.

Chapter 5: Result and Discussion. In this chapter, all the result and finding related to this study will be provided and discussed. An evaluation of the result and the discussion are explained in this chapter.

Chapter 6: Conclusion. This chapter is a last chapter of this thesis. This chapter presents the conclusion of the study. It consists of the benefit and weakness for this study. Besides, there are also suggested future enhancements that can be done.

REFERENCES

(n.d.). Retrieved from https://github.com/processone/ejjaberd

Alamin, A. A., & Mustafa, D. B. (2015). A Survey on Mobile Forensic for Android Smartphones. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 15-19.

Andriller Android Forensics Tools. (n.d.). Retrieved from Andriller Smartphone Forensics Decoder: https://www.andriller.com/decoders/

Anglano, C. (2014). Forensic Analysis of WhatsApp Messenger. *Digital Investigation Journal*, 201- 213.

Ejabberd: Build Awesome Realtime Software. (n.d.). Retrieved from ProcessOne: https://www.process-one.net/en/ejabberd/

Federal Investigation Agency National Response Centre for Cyber Crime. (n.d.). Retrieved from http://nr3c.gov.pk/cybercrime.html

Gudipaty LP, J. K. (2015). WhatsApp Forensics: Decryption of Encrypted WhatsApp Databases on. *J Inform Tech Softw Eng*.

Himanshu, S., & Tapaswi, S. (2015). Logical acquisition and analysis of data from android mobile devices. *Information & Computer Security*, 450- 475.

InfoSec Institute. (2017, May 26). Retrieved from http://resources.infosecinstitute.com/computer-forensics-tools/

Karpisek, F., Baggili. I., F. (2015). WhatsApp network Forensics: Decrypting and understanding the WhatsApp call signaling messages. Digital Investigation, 1- 9.

Le-Khac*, N.-A., Sgaras, C., & Kechadi, M.-T. (n.d.). Forensic Acquisition and Analysis of Tango VoIP.

Lone, A. H., Badroo, F. A., Chudhary, K. R., & Khalique, A. (2015). Implementation of Forensics Analysis Procedures for WhatsApp and Viber Android Applications. *International Journal of Computer Applications*.

Mahajan, A., Dahiya, M. S., & Sanghvi, H. P. (April 2013). Forensics Analysis of Instant Messenger Applications on Android Devices. *International Journal of Computer Applications*, 38- 44.

Mathavan, T., & Meeran, A. R. (2014). Acquisition and Analysis of Artifacts from Instant Messenger on Android Device. *International Journal of Engineering Research & Technology (IJERT)*.

Mayer, A. (2014, March 6). Retrieved from cbcnews Technology & Science: http://www.cbc.ca/news/technology/smartphones-becoming-prime-target-for-criminal-hackers-1.2561126

Mikhaylov, I. (2014). Extracting Data from Dump of Mobile Devices running Android Operating System. *Digital Frensics Articles and Research Papers Data Recovery, Hardware, Mobile Devices, Research, Software*.

Officers, A. O. (2012). ACPO Good Practice Guide. London, Police Cental e-Crime unit.

open handset alliance. (n.d.). Retrieved from https://www.openhandsetalliance.com/

Sahu, S. (2014). An Analysis of WhatsApp Forensics in Android Smartphone. *International Journal of Engineering Research*, 349- 350.

Satrya, G. (2016). Android Forensics Analysis: Private Chat on Social Messenger.

Satrya, G. B., Daely, P. T., & Shin, S. Y. (5-8 July 2016). Android forensics analysis: Private chat on social messenger. *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN).* Dublin, Ireland.

Schwartz, J. (2016, May 24). *NextLogik*. Retrieved from https://www.nextlogik.com/which-mobile-os-is-most-secure-ios-android-or-windows-slideshare/

Shortall, A., & Azhar, M. A. (2015). Forensics Acquisition of WhatsApp Data on Popular Mobile Platforms. *Sixth International Conference on Emerging Security Technologies*, 13-17.

Thakur, N. S. (2013). Forensics Analysis of WhatsApp on Android Smartphones.

Walker, J. (2017, Nov 16). *Digital Journal*. Retrieved from http://www.digitaljournal.com/tech-and-science/technology/nokia-android-smartphones-biggest-malware-target-in-2017/article/507775

Walnycky, D., Baggili, I., Marrington, A., Breitinger, F., & Moore, J. (2015). Network and Device Forensics Analysis of Android Social Messenging Applications. *The Digital Forensics Research Conference*