UNIVERSITI PUTRA MALAYSIA

WINDOWS 10 INSTANT MESSAGING APPLICATION FORENSICS

ALIYU USMAN SHEHU

FSKTM 2018 34

WINDOWS 10 INSTANT MESSAGING APPLICATION FORENSICS

By

ALIYU USMAN SHEHU

Thesis Submitted to Faculty of Computer Science and Information Technology,

Universiti Putra Malaysia,

In Fulfilment of the Requirements for the Degree of Master of Information Security

January 2018

COPYRIGHT

DEDICATION

This thesis is dedicated to my parents, for their infinite caring, prayers and support.

Favorite Quotes:

"The quieter you become, the more you can be able learn and hear" **Jalaluddin Rumi**

And

"Every contact leaves a trace" **Paul L. Kirk**

Abstract of Thesis presented to the Senate of University Putra Malaysia in Fulfillment of the requirement for the degree of Master of Information Security

WINDOWS 10 INSTANT MESSAGING APPLICATION FORENSICS

By

ALIYU USMAN SHEHU

JANUARY 2018

Supervisor: PROF MADYA DR. NUR IZURA UDZIR

Faculty: Computer Science and Information Technology

Abstract:

The way netizens communicate with each other deeper with the advent of Instant Messaging applications (IM apps). Thus, its flexibility and quick response on the IM apps has attracted the attentions of cybercriminal operations on the apps such as identity theft and phishing. The forensic investigation of instant messaging apps for the newest Windows 10 OS has been largely uninvestigated. Previous research dealt with dead analysis of the IM apps which did not guaranty accurate result for evidence. But, this research seeks to utilize the four stages of forensic investigation evidence: identification, collection, analysing and reporting. Furthermore, the study figured out data remnants from the top 1% Windows stores application software known as Facebook Instant Messaging apps on Windows 10 OS client machine. The research have focused on the volatile and nonvolatile artefacts with the aid of VM workstation version (VM) 9.0.0 build 812388 running Windows 10 (professional server pack1,64 bit, build 9600) while setting 2GB of physical memory and 20GB of hard disk. The research was be able to detect the kinds of terrestrial artefacts that are obtained after the use of Instant messaging services and software on the

contemporary Windows 10 OS. The findings from this research will contribute to the forensic community's understanding of types of terrestrial artefacts (login details, Installations, friend list, contacts, username, passwords, conversions etc.) which can be used on the establishment of evidence against the suspect on the court of law by forensic examiner.

Abstrak Tesis yang dikemukakan kepada Senat Universiti Putra Malaysia dalam Pemenuhan keperluan untuk ijazah Sarjana Keselamatan Maklumat

WINDOWS 10 FORENSICS APP MESSAGE INSTANT

Oleh

ALIYU USMAN SHEHU

Januari 2018

Penyelia: PROF MADYA DR. NUR IZURA UDZIR

Fakulti: Sains Komputer Dan Teknologi Maklumat

Cara netizens berkomunikasi dengan satu sama lain lebih mendalam dengan kedatangan aplikasi Pesanan Segera (aplikasi IM). Oleh itu, kelenturan dan tindak balas pantas terhadap aplikasi IM telah menangkap perhatian operasi jenayah siber di aplikasi seperti pencurian identiti dan pancingan data. Siasatan forensik aplikasi pemesejan segera untuk Windows 10 OS terbaru telah sebahagian besarnya tidak diperiksa. Penyelidikan sebelumnya menangani analisis mati aplikasi IM yang tidak menjamin hasil yang tepat untuk keterangan. Tetapi, kajian ini bertujuan untuk menggunakan empat peringkat bukti penyiasatan forensik: pengenalpastian, pengumpulan, analisa dan pelaporan. Tambahan pula, kajian ini menggambarkan sisa-sisa data dari perisian aplikasi Windows atas 1% yang dikenali sebagai aplikasi Instant Messaging Facebook pada mesin klien Windows 10 OS. kami akan memberi tumpuan kepada artifak yang tidak menentu dan tanpa voltan dengan bantuan versi workstation VM (VM) 9.0.0 membina 812388 yang menjalankan Windows 10 (pelayan profesional pack 1,64 bit, membina 9600) sambil menetapkan memori fizikal 2GB dan 20GB cakera. Penyelidikan ini akan dapat mengesan jenis artifak daratan yang diperolehi selepas penggunaan perkhidmatan dan perisian Pemesejan segera pada Windows 10 OS

kontemporari. Penemuan dari penyelidikan ini akan menyumbang kepada pemahaman masyarakat forensik mengenai jenis artifak terestrial (butiran log masuk, pemasangan, senarai rakan, kenalan, nama pengguna, kata laluan, penukaran) Yang boleh digunakan untuk penubuhan bukti terhadap suspek mahkamah undang-undang oleh pemeriksa forensik.

ACKWNOLEDGEMENTS

First and Foremost, I would like to express my sincere gratitude to my research supervisor Assoc. Prof. Dr. Nur Izura Udzir for continuous support of my study and research, for her patience, motivation, and immense knowledge. I would like to also show my deep gratitude to our Coordinator Asso. Prof. Dr. Nor. Fazlida Mohd Sani, and Dr. Mohd Taufik Abdullah, Dr. Izuan Hafez Hj. Ninggal, Hajah Zaiton Muda, Asso. Prof. Dr. Zuriati Ahmad Zukarnain and the entire Information Security lecturers. Without knowledge and assistance acquired from them, this thesis would have never been accomplished.

I will like to thank faculty of computer science and information technology for its supporting guidance and materials.

My endless appreciation goes to Ibrahim Badamasi Babangida University, Lapai, Niger State Nigeria for granting me scholarship with the aid of my mentor and Uncle Prof. Muhammad Nasir Maiturare who makes the processes achievable.

Getting through my thesis required more than academic support. To all my class mates and friends thank your understanding and encouragement.

Lastly but not the least, I am immensely grateful to my sheikh Professor Abdullah el-okene, Uncle Alhaji Yusuf Abdullahi Beji, Dr.Chindu Ibrahim Bisallah and my parents for unlimited love and support thought my life.

Alhamdulillahi Rabil Alamin.

DECLARTION

I hereby declare that the thesis is based on my original work excerpt for quotations and citation which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or any other institution.

ALIYU USMAN SHEHU

Date: 26 January, 2018

APPROVAL PAGE

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 of Information Security.

PROF MADYA DR. NUR IZURA UDZIR

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Supervisor)

Date: ……..

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVATIONS

API	Application Programming Interface
DD	Disk Dump
DFRWS	Digital Forensics Research Workshop
FTK	Forensic Tool Kit
IM	Instant Messaging
FTK	Forensic Tool Kit
RAM	Random Access Memory
SQL	Structured Query Language
TCP	Transmission Control Protocol
NTFS	New Technology File System
VM	Virtual Machine
VMDK	Virtual Machine Disk
VMEM	Virtual Memory
VMX	Virtual Machine Configuration File

CHAPTER 1

INTRODUCTION

1.1 Background

The popularity of Instant messaging (IM) for both mobile device users and novice computer users (i.e. personal computer and laptops) permit the exchange of information with peers in real time using text messaging, voice messaging and file sharing (Kabakus & Kara, 2015; Yang, Dehghantanha, Choo, & Muda, 2016). The wider range of IM users world-wide keep yielding from 5.8 billion to 8.3 billion between 2017 and 2021 (Pacific, 2017).

Contemporary to other client's technology, the IM services have been manipulated by cybercriminals in spreading malware, virus, committing scams and frauds and trap under 18 children's online to access adult contents. Moreover, unknown to the cybercriminals most of the activities on the machine can be traced and the conversion logs can be of great help to forensic examiner (Ochrymowicz, 2014; Yusoff, Mahmod, Dehghantanha, & Abdullah, 2014) on extracting the suspect's crime location, true identity, conversions, login details, and even online banking transactions details i.e. account number, username and passwords (Zhang & Choo, 2017) .

1.2 Problem Statement

It becomes an extensive challenge when to collect evidential data from IM Internet service provider (ISP) due to the increased-on user privacy requirements and demands for data redundancy (Barghuthi & Said, 2013; Kabakus & Kara, 2015). The protection of the data by encryption, protocols, Data protection Leakage (DLP) etc. make it harder to extract information from external network by forensic practitioners (Phillips & Steuart, 2016). Furthermore, the

ISP data privacy policies might be comprised, if forensic practitioner insist on collecting data from the Multi-Tenancy Environment. Moreover, even if the artefacts could be identified (Yang et al., 2016) the challenges still persist in terms of cross jurisdictional investigations which outlaw cross-border transfer of information (Dickson, 2006; Yusoff et al., 2014). Thus, its unacceptable for ISP to log on to their server to extract Suspect conversions due to increase on high traffic to the server(Joseph & Sunny, 2014). Alternatively, the user device can provide significant recovery methods of the IM artefacts which depends on IM application on action (Malik, Shashidhar, & Chen, n.d.; Stormo, 2013). Furthermore, in order to address the problem of evidence acquisition from ISP (Yang et al., 2016) the terrestrial artefacts could be significant on constructing whether a suspect has a direct connection to a crime, as the suspect may be a victim of phishing or identity theft. Thus, it's crucial for forensic investigator to be familiar with different techniques and what kinds of artefacts could be recoverable on the latest different types of IM apps(Quick, Choo, & Tassone, 2014; Yang et al., 2016). Based on this context, we seek to identify potential artefacts that may remain after the use of the Facebook windows store application software on Windows 10 user Machine. The research approach will follow that of (Quick & Choo, 2014; Quick et al., 2014; Yang et al., 2016) in order to establish accurate evidence.

1.3 Research Objectives

The research proposes to identify potential artefacts that may remain after the use of the Facebook windows store application software on Windows 10 user machine. The objectives of the research are provided as follows:

1. To determine what data remains in Random Access Memory (RAM) of the facebook application on a Windows 10 device.
2. To determine what data can be seen in the network traffic.

1.4 Research Questions

This section introduces the research questions to achieve the planned objectives of the research, for the purposes, a suitable methodology will be pursued to form the research, upon which the experiments will be based on. The research questions are defined as follows:

1.4.1 Research Questions 1.

To determine what data remains in Random Access Memory (RAM) of the facebook application on a Windows 10 device?

1.4.2 Research Question 2

To determine what data can be seen in the Network traffic?

1.5 Research Contributions

The finding from this research will contribute to the forensic community's understanding of types of terrestrial artefacts that are likely to remain after the use of Instant Messaging (IM) services and apps running on the latest Windows 10 operating system. Thus, to even the newest version to be released.

1.6 Research Scope

The scope of this research is to determine the data remnants on windows 10 PC for the use of facebook apps such as installation, logins, and conversions on transferred files, the research

aim at locating the network traffic on the RAM for better investigating and effective analysis in order to provide a guide to forensic examiners.

1.7 Thesis Structure

The organization of this thesis stated with abstract which indicate the summary of the research and advances with acknowledgement, approval page, declaration, list of figures, list of tables and list of abbreviations used in the thesis.

Chapter 1 Introduction: this gives the overview of Instant Messaging Application (IM) forensic investigations to widen the view on the topic to the reader. Background of the research is stated, as well as problem statement which shows the gap and reason of conducting the research. The objectives of the research is outlined. Concludely, the research scope and thesis organization are explained.

Chapter 2 Literature Review: This provide the latest literature review on this research. The chapter enclosed an outlined on windows 10 forensic, Digital forensic Investigation, Instant messaging windows forensics, facebook Instant Messaging apps forensic and Summary of the chapter is highlighted.

Chapter 3 Research Methodology This explained the research process, experimental design base on each research objectives. The Datasets of the research, research equipment's, forensic tools used on the forensic acquisitions and analysis are stated. Summary of the chapter is provided.

Chapter 4 Design and Analysis of Method: this chapter explained the forensic analysis carry out on the Designed method of the research in order to obtained accurate artifacts on both Victim and suspect machines for forensic analysis.

Chapter 5 Result and Discussions: In this chapter the results of Facebook Instant messaging applications forensics within windows 10 utilized the proposed method. The artifacts of data remnants found on the RAM and the Network traffic where documented with explanation for forensic examination reference. The chapter ends with findings of the forensic evidence.

Chapter 6 Conclusion: this showcase the summary of the research and thesis the detailed, the results, outcome of the results and Integrity of the evidence is presented. The implications and future enhancement of the research is highlighted.

REFERENCES

Alam, S., Aziz, M. A., & Iqbal, W. (2016). Forensic Analysis of Edge Browser In-Private Mode, *14*(9), 256–264.

Artifacts, W. (2016). KakaoTalk의 채팅 메시지 포렌식 분석 연구 및 WhatsApp의 Artifacts 와의 비교 분석, *20*(4), 777–785.

Ave, L. (2016).Patric [Windows 10 Forensics], Patric leahy center for Digital Investigation (802). retrieved https://www.cahamplain.edu

Barakat, A., & Hadi, A. (2016). Windows Forensic Investigations using PowerForensics Tool, 41–47. https://doi.org/10.1109/CCC.2016.18

Barghuthi, N. B. Al, & Said, H. (2013). Social Networks IM Forensics : Encryption Analysis, *8*(11), 708–715. https://doi.org/10.12720/jcm.8.11.708-715

Brockschmidt, K. (2012). Programming Windows 8 Apps with HTML, CSS, and JavaScript, 161. Retrieved from www.kraigbrockschmidt.com.

Chang, M. S. (2016). Forensic investigation of Amazon Cloud Drive on Windows 10, *3*(6), 478–482.

Chivers, H. (2014). Private browsing : A window of forensic opportunity. *Digital Investigation*, *11*(1), 20–29. https://doi.org/10.1016/j.diin.2013.11.002

Cortjens, D. (2012). Windows Live Messenger Forensics : Contact List Artefacts.

Dickson, M. (2006). An examination into AOL Instant Messenger 5 . 5 contact identification, *3*, 227–237. https://doi.org/10.1016/j.diin.2006.10.004

Domingues, P., & Frade, M. (2016). Digital Forensic Artifacts of the Cortana Device Search

Cache on Windows 10 Desktop. https://doi.org/10.1109/ARES.2016.44

Ibrahim, M., Abdullah, M. T., & Dehghantanha, A. (2012). Modelling Based Approach for Reconstructing Evidence of VoIP Malicious Attacks, *1*(4), 324–340.

Jason, S. (2015). Exposing vital forensic artifacts of USB devices in the Windows 10 registry NAVAL POSTGRADUATE.

Joseph, N., & Sunny, S. (2014). Volatile Internet Evidence Extraction from Windows Systems.

Kabakus, A. T., & Kara, R. (2015). Survey of Instant Messaging Applications Encryption Methods, *2*(4), 112–117.

Katz, M., Leo, H., Barrett, S., & Ave, L. (2014). iPhone Artifacts.

Lee, C., & Chung, M. (2015). Digital Forensic Analysis on Window8 Style UI Instant Messenger Applications, 1037–1042. https://doi.org/10.1007/978-3-662-45402-2

Malik, R., Shashidhar, N., & Chen, L. (n.d.). Analysis of Evidence in Cloud Storage Client Applications on the Windows Platform, 3–8.

Mushcab, R. Al, & Gladyshev, P. (2015). iPhone 5s Mobile Device, 146–151.

Ochrymowicz, R. (2014). Cloud-Based Storage Applications for Smart Phones : Forensic Investigation of Cloud Storage Applications Cloud-based storage applications for smart phones : Forensic investigation of cloud storage applications, (May).

Pacific, A. (2017). Instant Messaging Market, 2017-2021, *44*(0).

Phillips, A., & Steuart, C. (n.d.). *Guide to Computer Forensics and Investigations : Processing Digital Evidence Fifth Edition*.

Quick, D., & Choo, K. R. (2013a). Digital droplets : Microsoft SkyDrive forensic data

remnants. *Future Generation Computer Systems*, *29*(6), 1378–1394. https://doi.org/10.1016/j.future.2013.02.001

Quick, D., & Choo, K. R. (2013b). Dropbox analysis : Data remnants on user machines. *Digital Investigation*, *10*(1), 3–18. https://doi.org/10.1016/j.diin.2013.02.003

Quick, D., & Choo, K. R. (2014). Journal of Network and Computer Applications Google Drive : Forensic analysis of data remnants Digital Forensic Analysis Cycle. *Journal of Network and Computer Applications*, *40*, 179–193. https://doi.org/10.1016/j.jnca.2013.09.016

Quick, D., & Choo, K. R. (2016). Journal of Network and Computer Applications Pervasive social networking forensics : Intelligence and evidence from mobile device extracts. *Journal of Network and Computer Applications*, (November), 1–10. https://doi.org/10.1016/j.jnca.2016.11.018

Quick, D., Choo, K. R., & Tassone, C. (2014). Forensic Analysis of Windows Thumbcache files, *990*(July 2006), 1–13.

Singh, B., & Singh, U. (2016). A forensic insight into Windows 10 Jump Lists. *Digital Investigation*, *17*, 1–13. https://doi.org/10.1016/j.diin.2016.02.001

Singh, B., & Singh, U. (2017). A forensic insight into Windows 10 Cortana search. *Computers & Security*, *66*, 142–154. https://doi.org/10.1016/j.cose.2017.01.007

Stormo, J. M. (2013). Analysis of Windows 8 Registry Artifacts.

Studies, C. (2016). Network Traffic Forensics on Firefox Mobile OS : Facebook , Twitter , (November). https://doi.org/10.1016/B978-0-12-805303-4.00005-8

Teing, Y., Sc, B., Dehghantanha, A., Ph, D., Choo, K. R., & Ph, D. (2016). DIGITAL & MULTIMEDIA SCIENCES Forensic Investigation of Cooperative Storage Cloud

Service : Symform as a Case Study, (May). https://doi.org/10.1111/1556-4029.13271

Wong, K., Researcher, S., Lai, A. C. T., Yeung, J. C. K., & Lee, W. L. (2013). Facebook Forensics Finalized. *The Journal of Infectious Diseases*, *208*, NP. https://doi.org/10.1093/infdis/jis918

Yang, T. Y., Dehghantanha, A., Choo, K. R., & Muda, Z. (2016). Windows Instant Messaging App Forensics : Facebook and Skype as Case Studies, 1–29. https://doi.org/10.1371/journal.pone.0150300

Yusoff, M. N., Mahmod, R., Dehghantanha, A., & Abdullah, M. T. (2014). An Approach for Forensic Investigation in Firefox OS, 22–26.

Zhang, Z., & Choo, K. R. (2017). Guest Editorial : Multimedia Social Network Security and Applications, 3163–3168. https://doi.org/10.1007/s11042-016-4081-z