UNIVERSITI PUTRA MALAYSIA

ANALYTICAL METHOD FOR FORENSIC INVESTIGATION OF SOCIAL NETWORKING APPLICATIONS ON SMARTPHONES

FARHOOD NOROUZIZADEH DEZFOULI

FSKTM 2016 22

ANALYTICAL METHOD FOR FORENSIC INVESTIGATION OF SOCIAL NETWORKING APPLICATIONS ON SMARTPHONES

By

FARHOOD NOROUZIZADEH DEZFOULI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

May 2016

This thesis is dedicated to my parents

For their endless love, support, patience and encouragement

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

ANALYTICAL METHOD FOR FORENSIC INVESTIGATION OF SOCIAL NETWORKING APPLICATIONS ON SMARTPHONES

By

FARHOOD NOROUZIZADEH DEZFOULI

May 2016

Chairman : Ramlan Mahmod, PhD
Faculty : Computer Science and Information Technology

Social Networking has influenced the way people interact with each other. Many people use social networking applications for individual or commercial purposes to share information. However, the rapid growth of social networking and social networking applications on mobile devices has attracted cyber criminals and has resulted in their use in many criminal activities such as identity theft, piracy, illegal trading, sexual harassment, cyber stalking and cyber terrorism. Mobile devices are a gold mine of evidences for forensic investigators as they store valuable social networking data.

Previous researches on forensic investigation of social networking applications on smartphones were conducted using existing forensic analyzer tools and failed to identify important data remnants including passwords, GPS locations, uploaded files, posts and messages. Therefore, the result of previous researches indicate that the current mobile forensic analyzer tools and methods are not able to automatically acquire enough valuable data remnants from social networking applications on smartphones and only provide an interface to the data for the investigator.

In this research, we propose an examination method for investigation of social networking applications on smartphones in order to detect all possible data remnants when undertaking the forensic investigation of social networking platforms. In this examination method, logical and physical images of smartphones are examined manually using a set of predefined keywords. This will allow the investigators to detect the data remnants and identify their patterns. The identified patterns are then used to design an algorithm for detecting social networking data remnants automatically.

The outcome of this research resulted in detection of user's username, password, *UID*, personal information, pictures, workplace and organization, GPS locations, friend list, uploaded posts, uploaded messages, uploaded comments, uploaded files, interests and identification of the pattern for how and where each data remnant is stored in the

internal memory and internal storage of the smartphone. Moreover, an algorithm was designed that automatically extracts social networking data remnants from smartphones using the identified patterns.

We hope this research can be a stepping stone for identifying a common methodology for investigation of all types of smartphone applications and serve as the first step toward developing a consistent digital forensic framework for social networking such as the one proposed and evaluated in this research.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

KAEDAH ANALITIK UNTUK PENYIASATAN FORENSIK KE ATAS APLIKASI RANGKAIAN SOSIAL DALAM TELEFON PINTAR

Oleh

FARHOOD NOROUZIZADEH DEZFOULI

Mei 2016

Pengerusi : Ramlan Mahmod, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Rangkaian Sosial telah mempengaruhi cara orang berinteraksi antara satu sama lain. Ramai orang menggunakan aplikasi rangkaian sosial untuk tujuan individu atau komersial untuk berkongsi maklumat. Walau bagaimanapun, pertumbuhan pesat rangkaian sosial dan aplikasi rangkaian sosial pada peranti mudah alih telah menarik penjenayah siber dan telah menyebabkan penggunaannya dalam pelbagai aktiviti jenayah seperti kecurian identiti, cetak rompak, perdagangan haram, gangguan seksual, ugutan siber dan keganasan siber. Peranti mudah alih adalah sebuah lombong emas bukti-bukti bagi penyiasat forensik kerana ia menyimpan data rangkaian sosial berharga.

Kajian terdahulu mengenai penyiasatan forensik aplikasi rangkaian sosial pada telefon pintar telah dijalankan dengan menggunakan alat penganalisis forensik sedia ada dan gagal untuk mengenal pasti sisa-sisa data penting termasuk kata laluan, lokasi GPS, fail yang dimuatnaik, pos dan mesej. Oleh itu, hasil daripada kajian terdahulu menunjukkan bahawa alat-alat penganalisis forensik mudah alih semasa dan kaedah tidak dapat memperoleh sisa-sisa data penting yang cukup dari aplikasi rangkaian sosial secara automatik pada telefon pintar dan hanya mehyediakan antara muka kepada data untuk penyiasat.

Dalam kajian ini, kami mencadangkan satu kaedah pemeriksaan untuk siasatan aplikasi rangkaian sosial pada telefon pintar untuk mengesan semua kemungkinan sisa-sisa data apabila menjalankan siasatan forensik platform rangkaian sosial. Dalam kaedah pemeriksaan ini, imej logik dan fizikal telefon pintar diperiksa secara manual menggunakan satu set kata kunci yang telah ditetapkan. Ini akan membolehkan penyelidik untuk mengesan saki-baki data dan mengenal pasti corak mereka. Corak yang dikenal pasti kemudiannya digunakan untuk mereka bentuk algoritma untuk mengesan saki-baki data rangkaian sosial secara automatik.

Hasil kajian ini menghasilkan nama pengguna, kata laluan, *UID*, maklumat peribadi, gambar, tempat kerja dan organisasi, lokasi *GPS*, senarai rakan, pos yang dimuat naik,

mesej yang dimuat naik, komen yang dimuat naik, fail yang dimuat naik, minat dan pengenal pastian bentuk bagaimana setiap sisa data disimpan dalam memori dalaman dan storan dalaman telefon pintar. Selain itu, algoritma telah direka secara automatik mengeluarkan sisa data rangkaian sosial daripada telefon pintar menggunakan bentuk yang dikenal pasti.

Kami berharap kajian ini boleh menjadi batu loncatan untuk mengenal pasti suatu kaedah sepunya untuk melakukan penyiasatan ke atas semua jenis aplikasi telefon pintar dan berfungsi sebagai langkah pertama ke arah membangunkan rangka kerja forensik digital yang konsisten untuk rangkaian sosial seperti yang dicadangkan dan dinilai dalam kajian ini.

AKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to my research supervisor Professor Dr. Ramlan Mahmod for the continuous support of my study and research, for his patience, motivation, and immense knowledge. I would also like to show gratitude to my supervisory committee, including Assoc. Prof. Dr. Nor Fazlida Mohd Sani, and Dr. Solahuddin bin Shamsuddin. Without their assistance and dedicated involvement in every step throughout the process, this thesis would have never been accomplished.

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

Getting through my thesis required more than academic support. To all my friends, thank you for your understanding and encouragement.

Last but not least, I am immensely grateful to my parents for their unlimited love and support throughout my life.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science.

The members of the Supervisory Committee were as follows:

Ramlan Mahmod, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Nor Fazlida Mohd Sani, PhD
Associate. Professor
Fsculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Solahuddin Bin Shamsuddin, PhD
Chief Technology Officer
Cyber Security Malaysia
(Member)

BUJANG KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by the 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 Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____ Date: _____

Name and Matric No.: Farhood Norouzizadeh Dezfouli / GS33111

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: _____
Name of Chairman of Supervisory Committee: _____

Signature: _____
Name of Member of Supervisory Committee: _____

Signature: _____
Name of Member of Supervisory Committee: _____

TABLE OF CONTENTS

		Page
ABSTRACT		i
ABSTRAK		iii
AKNOWLEDGEMENTS		v
APPROVAL		vi
DECLARATION		viii
LIST OF TABLES		xii
LIST OF FIGURES		xiii
LIST OF ABBREVIATIONS		xv
CHAPTER		
1	**INTRODUCTION**	**1**
	1.1 Background	1
	1.2 Problem Statement	2
	1.3 Research Objectives	3
	1.4 Research Scope	4
	1.5 Thesis Organization	4
2	**LITERATURE REVIEW**	**6**
	2.1 Introduction	6
	2.2 Social Networking	6
	2.3 Digital Forensic Investigation	8
	2.4 Social Networking and Digital Forensic	12
	2.5 Mobile Device Forensic	13
	2.6 Social Networking and Mobile Forensic	15
	2.7 Current Related Researches	15
	2.7.1 Digital Forensic OSN Model	15
	2.7.2 SN Apps Investigation On Computers	16
	2.7.3 SN Apps Investigation On Smartphones	16
	2.8 Summary	18
3	**RESEARCH METHODOLOGY**	**20**
	3.1 Introduction	20
	3.2 Research Process	20
	3.3 Experiment Design	21
	3.3.1 Data Set	21
	3.3.2 Experiment Process	22
	3.4 Research Equipment	29
	3.5 Summary	30
4	**SMARTPHONE SOCIAL NETWORKING EXAMINATION METHOD**	**31**
	4.1 Introduction	31
	4.2 Adopted Digital Forensic Framework	31
	4.2.1 Scoping	32
	4.2.2 Identification and Preparation	33

4.2.3 Collection 33
4.2.4 Preservation 33
4.2.5 Examination and Analysis 33
4.2.6 Presentation 39
4.2.7 Report 39
4.3 Discussion 39
4.4 Summary 41

5 RESULTS AND DISCUSSION 42
5.1 Introduction 42
5.2 Android Examination 42
5.2.1 Scoping 42
5.2.2 Identification and Preparation 43
5.2.3 Collection 43
5.2.4 Preservation 45
5.2.5 Examination and Analysis 45
5.2.6 Presentation 65
5.2.7 Report 69
5.3 iOS Examination 69
5.3.1 Scoping 69
5.3.2 Identification and Preparation 70
5.3.3 Collection 70
5.3.4 Preservation 71
5.3.5 Examination and Analysis 71
5.3.6 Presentation 87
5.3.7 Report 91
5.4 Summary of Findings 91
5.4.1 Data Remnants Analysis and Comparison 91
5.5 Summary 94

6 CONCLUSION AND FUTURE WORK 95
6.1 Introduction 95
6.2 Conclusion 96
6.3 Future Works 97

REFERENCES 98
BIODATA OF STUDENT 103
LIST OF PUBLICATIONS 104

LIST OF TABLES

Table		Page
3.1	User Details and Sample Data for Android Experiments	24
3.2	User Details and Sample Data for iOS Experiments	25
3.3	List of software used in the research	29
3.4	List of hardware used in the research	30
4.1	List of keyword search terms for identifying user credentials	34
4.2	List of keyword search terms for identifying common activities	35
4.3	List of common forensic tools used in previous researches	40
4.4	Performance measurement	40
5.1	Summary of findings in Android's internal memory	67
5.2	Summary of findings in Android's internal storage	67
5.3	Summary of findings in Android's network traffic	69
5.4	Summary of findings in iOS backup	89
5.5	Summary of findings in iOS's network traffic	91
5.6	Comparison of data remnants of the social networking applications on smartphones	92

LIST OF FIGURES

Figure		Page
2.1	Percentage of Internet users who use social networking, by age group	8
2.2	Zainudin's model for forensic investigation of online social networking	16
3.1	Research process steps	20
3.2	Research experimental design	22
3.3	Block Diagram of Research Scope for Android and iOS	23
3.4	Actions carried out for each scenario in Android and iOS experiment	27
4.1	SSNFF digital forensics investigation framework	32
4.2	Proposed examination method	34
4.3	Examination algorithm for investigating SN apps on smartphones	37
4.4	Pseudocode of the examination algorithm	38
5.1	Collection of physical image from internal memory of Android device	44
5.2	Collection of physical image from internal storage of Android device	45
5.3	Facebook username and password artifact in Android	46
5.4	Facebook login artifact in Android	47
5.5	Facebook user's personal information artifact in Android	48
5.6	Facebook user's friend list artifact in Android	48
5.7	Facebook user's GPS location artifact in Android	48
5.8	Facebook user's interests artifact in Android	49
5.9	Facebook uploading posts artifact in Android	49
5.10	Facebook photo upload artifact in Android	50
5.11	Facebook instant messaging artifact in Android	50
5.12	Facebook uploading comments artifact in Android	51
5.13	Facebook network traffic artifact in Android	51
5.14	Facebook username and password artifact in Android	52
5.15	Twitter login artifact in Android	53
5.16	Twitter user's personal information artifact in Android	53
5.17	Twitter uploading posts artifact in Android	54
5.18	Twitter photo upload artifact in Android	54
5.19	Twitter instant messaging artifact in Android	55
5.20	Twitter uploading comments artifact in Android	55
5.21	Twitter network traffic artifact in Android	56
5.22	LinkedIn username and password artifact in Android	57
5.23	LinkedIn login artifact in Android	57
5.24	LinkedIn user's personal information artifact in Android	58
5.25	LinkedIn uploading posts artifact in Android	59
5.26	LinkedIn instant messaging artifact in Android	59
5.27	LinkedIn uploading comments artifact in Android	60

5.28	LinkedIn network traffic artifact in Android	61
5.29	Google+ username and password artifact in Android	61
5.30	Google+ login artifact in Android	62
5.31	Google+ user's personal information artifact in Android	63
5.32	Google+ uploading posts artifact in Android	63
5.33	Google+ instant messaging artifact in Android	64
5.34	Google+ uploading comments artifact in Android	64
5.35	Google+ network traffic artifact in Android	65
5.36	Collection of physical image from internal storage of iOS device	71
5.37	Facebook login artifact in iOS	72
5.38	Facebook user's personal information artifact in iOS	73
5.39	Facebook uploading posts URL artifact in iOS	73
5.40	Facebook instant messaging timestamp in iOS	74
5.41	Facebook instant messaging artifact in iOS	74
5.42	Facebook uploading comments artifact in iOS	75
5.43	Facebook network traffic artifact in iOS	76
5.44	Twitter login artifact in iOS	77
5.45	Twitter user's profile information artifact in iOS	77
5.46	Twitter uploading posts artifact in iOS	78
5.47	Twitter instant messaging artifact in iOS	78
5.48	Twitter uploading comments artifact in iOS	78
5.49	Twitter network traffic artifact in iOS	79
5.50	LinkedIn login artifact in iOS	80
5.51	LinkedIn user's personal information artifact in iOS	81
5.52	LinkedIn uploading posts artifact in iOS	81
5.53	LinkedIn instant messaging artifact in iOS	82
5.54	LinkedIn uploading comments artifact in iOS	82
5.55	LinkedIn network traffic artifact in iOS	83
5.56	Google+ login artifact in iOS	84
5.57	Google+ user's personal information artifact in iOS	84
5.58	Google+ uploading posts artifact in iOS	85
5.59	Google+ network traffic artifact in iOS	86

LIST OF ABBREVIATIONS

ACPO	Association of Chief Police Officers
ADB	Android Debug Bridge
ADFM	Abstract Digital Forensics Model
CFSAP	Computer Forensic - Secure, Analyze, Present
CPU	Central Processing Unit
DD	Disk Dump
DFRWS	Digital Forensic Research Workshop
EDRM	Electronic Discovery Reference Model
ESI	Electronically Stored Information
FTK	Forensic Tool Kit
GPS	Global Positioning System
IM	Internal Memory
iOS	Apple iPhone Operating System
IP	Internet Protocol
IS	Internal Storage
MD5	Message Digest 5
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
NT	Network Traffic
OS	Operating System
OSN	Online Social Network
PC	Personal Computer
PCAP	Network traffic capture file
PLIST	Property List
SANS	System Administration, Networking, and Security
SHA1	Secure Hash Algorithm 1
SN	Social Networking
SSH	Secure Shell
SSNFF	Smartphone Social Networking Forensic Framework
SWGDE	Scientific Working Group on Digital Evidence
UID	User Identification
URL	Uniform Resource Locator
USB	Universal Serial Bus

CHAPTER 1

INTRODUCTION

1.1 Background

Boyd & Ellison (2007), defined social network (SN) sites as web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system.

Currently, there are hundreds of social networking sites available on the Internet. As the time of writing, Facebook is the most popular social networking site with around 1.06 billion active users monthly (Cross, 2013). Other popular social networking sites include Twitter, LinkedIn and Google+.

Facebook, Twitter, LinkedIn and Google+ provide users with features such as email, blogging, instant messaging and photo sharing for social and commercial exchange (Taylor et al., 2014). Various types of personal information are shared in social networking sites by users including full name, date of birth, pictures, email address, phone number, gender, group affiliations and even name of family members (Kisekka et al., 2013).

Over the past few years, advancement in mobile devices technology and social networking sites enabled users to use these devices in order to connect to social networking sites. Many social networking sites have developed applications which users can obtain from App Stores or Web sites. Once the application is installed on the mobile device, it provides an interface to features of the social networking site. For instance, Facebook application enables users to view their profile page, review their news feed and update their status from their mobile devices. These applications display the content of the social networking sites on the device in a format specifically for mobile users. A survey conducted by Pew Internet & American Life Project (2013), indicated that 40% of mobile device users access social networking sites on their devices and 28% of them do so every day.

The rapid growth of social networking has also attracted cyber criminals and has resulted in their use in many criminal activities such as identity theft, piracy, illegal trading, sexual harassment, cyber stalking and cyber terrorism (Zainudin et al., 2010).

Forensic is the science of using techniques and tools to gather evidence for civil and criminal trials (Cross, 2013). Subsequently, *Digital Forensic* is a branch of *Forensic*

science which focuses on the process of identification, preservation, collection and examination of evidence in relation to digital media such as computers, mobile devices, networks and other digital sources (Cross, 2013).

The increased use of social networks and social networking applications on mobile devices raises the importance of digital forensic in this area. Mobile devices might contain valuable digital evidences regarding a case involving social networking applications and these evidences can be recovered with the use of correct tools and examination methods (Baca et al., 2013).

A significant issue faced by forensic investigators when undertaking forensic examination of social networking applications on mobile devices is the lack of a theoretical framework that guides the process of investigation. Using ad-hoc processes and tools to extract digital evidence can jeopardize the integrity and credibility of evidence since in courts and criminal prosecution both the evidence and the processes used for obtaining it can be the subject of questions (Zainudin et al., 2010).

The motivation in conducting research in the field of social networking and mobile devices can be summarized in following three points; every day the number of mobile device users who access social networking sites is increasing. Criminals have realized this increase and are using mobile devices to conduct criminal activities in social networks such as identity theft, cyber stalking and cyber terrorism. Forensic investigation of mobile devices regarding social networking applications is limited since there is no complete examination method to guide the process of investigation (Zainudin et al., 2010).

1.2 Problem Statement

In the recent researches, Zainudin et al. (2010) proposed a model for forensic investigation of online social networks which consists of four phases namely Preliminary, Investigation, Analysis and Evaluation. The model discusses the online searching of users' profiles to identify the links between users. Said et al. (2011) examined Facebook and Twitter on iPhone 3GS, BlackBerry Bold and Samsung Omnia II 18000. In their research, a logical method of acquisition was used to acquire backups from each device and forensic investigation of each application was carried out using various tools such as plist Editor, SQLite Database Browsers and Mobiledite Forensic. The researchers extracted user's login email and login time from Facebook application and user's tweets and public profiles visited from Twitter application on iPhone 3GS. However, they could not recover any related data remnants to the use of Facebook and Twitter applications on BlackBerry and Samsung devices. Al Mutawa et al. (2012) investigated Facebook, Twitter and MySpace applications on an iPhone 4, Blackberry Torch 9800 and Samsung GT-i9000 Galaxy S, and used a logical acquisition technique to conduct the investigation. They utilized some forensic tools such as EnCase to investigate the internal storage of the smartphones and extracted user's personal data, uploaded photos and posted comments from iPhone and the Samsung Galaxy. However, their research did not report any data remnants from BlackBerry device.

In order to identify the gap of the research, the model proposed by Zainudin et al. (2010) only discusses the investigation of users' profile through the online interface of the social networks and does not include the investigation of computers or smartphones in order to determine what type of data remnants may remain on these devices. In terms of data remnants, the method used in the research of Said et al. (2011) did not result in extraction of any significant data remnants from the backup files except for username and login time and the content of most of the backup files could not be identified. The research of Al Mutawa et al. (2012) retrieved significant data remnants such as username and uploaded posts from the smartphones regarding social networking applications. Although, there are still several important data remnants such as passwords, location data and uploaded files which could not be recovered using the method used in that research. Therefore, there is a need for an examination method that has the capability to identify and retrieve all possible social networking data remnants including the ones missed in previous researches such as passwords, location data and uploaded files while allows the investigators to understand where the data remnants are stored on the smartphone and how they can be extracted. The target of the investigation in this research is to identify all possible SN data remnants on smartphones including the data remnants that were missed in previous researches. The outcome of the investigation is to detect user's username, password, *UID*, personal information, pictures, work and education, GPS locations, friend list, uploaded posts, uploaded messages, uploaded comments, uploaded files, interests and to identify the pattern for how each data remnant is stored on the internal memory and internal storage of the smartphone.

Furthermore, previous researches use common mobile forensic tools to perform examination on smartphones in order to detect and extract data remnants of social networking applications. There are several variety of mobile forensic tools. While some tools provide acquisition capabilities, they do not provide examination or reporting facilities (Ayers et al., 2014). Moreover, every tool does not support all smartphones and operating systems and each tool supports only a limited number of devices (Ayers et al., 2007). In addition, mobile forensic tools do not automatically perform examination on collected data from the smartphones and only provide an interface for manual examination by the investigator (Thomas et al., 2010; Goel et al., 2012). The researches of Said et al. (2011) and Al Mutawa et al. (2012) indicate that the current mobile forensic analyzer tools and methods are not able to automatically extract enough valuable data remnants from social networking applications on smartphones. As the result, previous researches failed to identify important data remnants including passwords, GPS locations, uploaded files, posts and messages. Therefore, there is a need for an algorithm to be developed that allows automatic extraction of data remnants from SN apps on smartphones which enhances the process of performing digital forensic investigation on smartphones in terms of accuracy and efficiency.

1.3 Research Objectives

The objective of this research is to design an examination method for forensic investigation of social networking applications on Android and iOS devices. Therefore, the sub-objectives of the research are as follows.

Sub-objective 1: To propose an examination method for digital forensic investigation of social networking applications on smartphones including Android and iOS platforms in order to detect all possible data remnants when undertaking the forensic investigation of social networking platforms including Facebook, Twitter, LinkedIn and Google+.

Sub-objective 2: To design an algorithm for automation of extraction and examination phase in digital forensic investigation of social networking platforms namely Facebook, Twitter, LinkedIn and Google+ applications on smartphones including Android and iOS devices.

1.4 Research Scope

The research was undertaken using Android version 4.2 and iOS version 7.1.2 for smartphones. Alternative operating systems and their versions may all have different outcomes and data remnants. Additionally, the research was limited to the most popular social networking applications of Facebook, Twitter, LinkedIn and Google+ at the time of undertaking this study. However, any other application may have different results and findings. Additionally, the research was undertaken using the proposed forensics examination method on the smartphones components of internal memory and the internal storage. However, the network traffic of the devices was analyzed using the existing forensics tools.

This research was limited to rooted Samsung Galaxy Tab II, 16 GB, and a jailbroken iPhone 5s with 32GB internal storage. However, nonjailbroken devices may provide different outcomes and information. Android and iOS devices normally do not allow access to the system files. This means that the file system is restricted and cannot be seen by the user. Therefore, acquiring a physical bit-by-bit image from the internal memory and internal storage of the devices is not possible. Thus, to obtain these, it was necessary to root or jailbreak the devices first in order to get access to the file systems. For the Android device in hand for this research, the CF-Root method was used. The reason for choosing this method is that CF-Root keeps the device's firmware as close to stock as possible (Akmal, 2014). This means that this method applies the least amount of modification to the device's firmware and file system. For the iOS device in hand for this research, the Pangu freeware was used. The reason for choosing Pangu is that aside from Cydia, it does not install any other third party application on the iOS device (Esposito, 2014).

1.5 Thesis Organization

This thesis begins with an abstract which provides a brief summary of the research and continues with acknowledgments, approval, declaration, list of figures, list of tables and list of abbreviations used in the thesis.

Chapter One – Introduction begins with background which provides information about social networking and digital forensic investigation in order to introduce the

topic of the research to reader. Background is followed by problem statement where the gap of research and the reason for conducting this research is described. Then, the objectives of the research are outlined. Finally, research scopes are highlighted and structure of the thesis is explained.

Chapter Two – Literature Review provides a review of current literature relevant to this research. This chapter provides an outline on social networking, digital forensic examination and social networking applications on mobile devices. Existing issues in forensic examination of social networking applications on mobile devices are highlighted and a summary concludes the chapter.

Chapter Three – Research Methodology explains the nature of the research and outlines the research steps. Research methodology for each research objective and experiment process are described in detail along with the dataset used for experiments. Finally, equipment and software used for research experiments are listed and the chapter is concluded.

Chapter Four – Proposed model describes the proposed examination method for investigation of social networking application on smartphones and explains how this method could be applied to digital forensic investigation of smartphones when social networking application are involved. Phases of the adopted digital forensic framework (Scope, Identification and Preparation, Collection, Preservation, Examination and Analysis, Presentation, and Report) are explained. The proposed examination method is presented and discussed in detail and summary of the chapter is provided.

Chapter Five – Results and Discussion presents the examination of Facebook, Twitter, LinkedIn and Google+ social networking application within Android and iOS devices utilizing the proposed examination method. Examination is undertaken to determine the data remnants of each application. Afterwards, results and findings of the examination are presented and discussed and the chapter is concluded with the summary.

Chapter Six – Conclusion and Future Work provides a summary of the research and thesis. First, a brief summary of what has been done throughout the thesis is provided and then the results and outcomes of the research are presented. Finally, validity, implications of the research and future research opportunities are discussed.

REFERENCES

ACPO. (2011). Good Practice Guide for Computer-Based Electronic Evidence. Association of Chief Police Officers.

Akmal, T. (2014). Root XXU1AOCV Android 5.0.2 Lollipop on Galaxy S6 G920F Official Firmware - Tutorial / Guide. Retrieved from http://www.teamandroid.com/2015/04/27/root-xxu1aocv-android-502-lollipop-galaxy-s6-g920f-official-firmware/

Al Mutawa, N., Al Awadhi, I., Baggili, I., & Marrington, A. (2011). Forensic artifacts of Facebook's instant messaging service. In *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for* (pp. 771–776).

Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation*, *9*, S24–S33. http://doi.org/10.1016/j.diin.2012.05.007

Alghafli, K. A., Jones, A., & Martin, T. A. (2011). Guidelines for the digital forensic processing of smartphones. In *in the Proceedings of the 9th Australian Digital Forensics Conference*. Perth Western Australia: Edith Cowan University.

Angelopoulou, O., & VIDALIS, S. (2013). Towards "Crime Specific" Digital Investigation Frameworks. Presented at the The 3rd International Conference on Cybercrime, Security and Digital Forensics, School of Computer Science, University of Cardiff, Cardiff.

Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on mobile device forensics* (No. NIST SP 800-101r1). National Institute of Standards and Technology.

Ayers, R. P., Jansen, W., Delaitre, A. M., & Moenner, L. (2007, March 21). Cell Phone Forensic Tools: An Overview and Analysis Update. US Department of Commerce.

Baca, M., Cosic, J., & Cosic, Z. (2013). Forensic analysis of social networks (case study). In *Information Technology Interfaces (ITI), Proceedings of the ITI 2013 35th International Conference on* (pp. 219–223). IEEE.

Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013). A critical review of 7 years of Mobile Device Forensics. *Digital Investigation*, *10*(4), 323–349. http://doi.org/10.1016/j.diin.2013.10.003

Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. http://doi.org/10.1111/j.1083-6101.2007.00393.x

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press.

Church, E., & Fafinski, S. (2011). Social networks, crime and the law. *Student Law Review*, 13–16.

Cisco, T. (2013). Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017. *Cisco Public Information*.

Cross, M. (2013). *Social Media Security: Leveraging Social Networking While Mitigating Risk* (1st edition). USA: Syngress.

Damopoulos, D., Kambourakis, G., & Gritzalis, S. (2011). iSAM: An iPhone Stealth Airborne Malware. In J. Camenisch, S. Fischer-Hübner, Y. Murayama, A. Portmann, & C. Rieder (Eds.), *Future Challenges in Security and Privacy for Academia and Industry* (pp. 17–28). Springer Berlin Heidelberg.

Damopoulos, D., Kambourakis, G., & Gritzalis, S. (2013). From keyloggers to touchloggers: Take the rough with the smooth. *Computers & Security*, *32*, 102–114.

Damopoulos, D., Kambourakis, G., Gritzalis, S., & Park, S. O. (2012). Exposing mobile malware from the inside (or what is your mobile app really doing?). *Peer-to-Peer Networking and Applications*, 1–11.

EDRM LLC, EDRM Enron Email Data Set. (2013). Retrieved January 7, 2014, from http://www.edrm.net/resources/data-sets/edrm-enron-email-data-set

Esposito, D. (2014). How to jailbreak iOS 7.1 and 7.1.x with Pangu (Video). Retrieved from http://9to5mac.com/2014/06/23/how-to-jailbreak-ios-7-1-and-7-1-1-with-pangu-video/

Goel, A., Tyagi, A., & Agarwal, A. (2012). Smartphone Forensic Investigation Process Model. *International Journal of Computer Science & Security (IJCSS)*, *6*(5), 322–341.

Howden, C., Liu, L., Ding, Z., Zhan, Y., & Lam, K. P. (2013). Moments in Time: A Forensic View of Twitter (pp. 899–908). IEEE. http://doi.org/10.1109/GreenCom-iThings-CPSCom.2013.157

Hutchings, C. (2012). Commercial use of Facebook and Twitter – risks and rewards. *Computer Fraud & Security*, *2012*(6), 19–20. http://doi.org/10.1016/S1361-3723(12)70065-9

Jung, J., Jeong, C., Byun, K., & Lee, S. (2011). Sensitive Privacy Data Acquisition in the iPhone for Digital Forensic Analysis. In J. J. Park, J. Lopez, S.-S. Yeo, T. Shon, & D. Taniar (Eds.), *Secure and Trust Computing, Data Management and Applications* (pp. 172–186). Springer Berlin Heidelberg.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59–68. http://doi.org/10.1016/j.bushor.2009.09.003

Kisekka, V., Bagchi-Sen, S., & Raghav Rao, H. (2013). Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users. *Computers in Human Behavior*, *29*(6), 2722–2729. http://doi.org/10.1016/j.chb.2013.07.023

Lessard, J., & Kessler, G. (2009). Android Forensics: Simplifying Cell Phone Examinations. *Small Scale Digital Device Forensics Journal*, *4*(1). Retrieved from http://ro.ecu.edu.au/ecuworks/6479/

McKemmish, R. (1999). What is forensic computing? *Trends & Issues in Crime and Criminal Justice*, (118), 1–6.

Mohay, G. M., Anderson, A., Collie, B., McKemmish, R. D., & Vel, O. de. (2003). *Computer and Intrusion Forensics*. Norwood, MA, USA: Artech House, Inc.

NIJ. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. US Department of Justice, Office of Justice Program, National Institute of Justice.

NIJ. (2008). *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*. US Department of Justice, Office of Justice Program, National Institute of Justice.

NIST. (2006). *Guide to Integrating Forensic Techniques into Incident Response* (No. NIST SP 800-86). National Institute of Standards and Technology.

Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior*, *26*(3), 406–418. http://doi.org/10.1016/j.chb.2009.11.012

Palmer, G. (2001). *2001-A Road Map for Digital Forensic Research.pdf*. Digital Forensic Research Work Group (DFRWS).

Pew Internet & American Life Project. (2013). Social Networking Fact Sheet. Retrieved from http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/

Pritchett, S. (2011). How do employers protect data from theft by their employees? *Privacy and Data Protection*, *11*(5), 8–14.

Quick, D., & Choo, K.-K. R. (2013a). Digital droplets: Microsoft SkyDrive forensic data remnants. *Future Generation Computer Systems*, *29*(6), 1378–1394. http://doi.org/10.1016/j.future.2013.02.001

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

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

Raghavan, S. (2013). Digital forensic research: current state of the art. *CSI Transactions on ICT*, *1*(1), 91–114. http://doi.org/10.1007/s40012-012-0008-7

Ratcliffe, J. (2003, April). Intelligence-led policing [Pamphlet]. Retrieved October 28, 2014, from http://aic.gov.au/publications/current%20series/tandi/241-260/tandi248.html

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, *1*(3), 1–12.

Said, H., Yousif, A., & Humaid, H. (2011). IPhone forensics techniques and crime investigation. In *Current Trends in Information Technology (CTIT), 2011 International Conference and Workshop on* (pp. 120–125). IEEE.

Sipior, J. C., Ward, B. T., Volonino, L., & MacGabhann, L. (2013). A Framework for the E-Discovery of Social Media Content in the United States. *Inf. Sys. Manag.*, *30*(4), 352–358. http://doi.org/10.1080/10580530.2013.832965

Slay, J., Lin, Y.-C., Turnbull, B., Beckett, J., & Lin, P. (2009). Towards a Formalization of Digital Forensics. In G. Peterson & S. Shenoi (Eds.), *Advances in Digital Forensics V* (Vol. 306, pp. 37–47). Berlin, Heidelberg: Springer Berlin Heidelberg.

Spaulding, T. J. (2010). How can virtual communities create value for business? *Electronic Commerce Research and Applications*, *9*(1), 38–49. http://doi.org/10.1016/j.elerap.2009.07.004

Stephenson, P. (2003). Modeling of Post-Incident Root Cause Analysis. *International Journal of Digital Evidence*, *2*(2).

SWGDE. (2011). SWGDE and SWGIT Digital and Multimedia Evidence Glossary. Scientific Working Group on Digital Evidence.

Taylor, M., Haggerty, J., & Gresty, D. (2007). The legal aspects of corporate computer forensic investigations. *Computer Law & Security Review*, *23*(6), 562–566. http://doi.org/10.1016/j.clsr.2007.09.002

Taylor, M., Haggerty, J., Gresty, D., Almond, P., & Berry, T. (2014). Forensic investigation of social networking applications. *Network Security*, *2014*(11), 9–16. http://doi.org/10.1016/S1353-4858(14)70112-6

Thomas, P., Owen, P., & McPhee, D. (2010). An Analysis of the Digital Forensic Examination of Mobile Phones. In *Fourth International Conference on Next Generation Mobile Applications* (pp. 25–29). IEEE. http://doi.org/10.1109/NGMAST.2010.17

Tso, Y.-C., Wang, S.-J., Huang, C.-T., & Wang, W.-J. (2012). iPhone Social Networking for Evidence Investigations Using iTunes Forensics. In *Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication* (pp. 62:1–62:7). New York, NY, USA: ACM. http://doi.org/10.1145/2184751.2184827

Waggoner, K. (Ed. . (2007). Handbook of Forensic Services. Federal Bureau of Investigation.

Weir, G. R. S., Toolan, F., & Smeed, D. (2011). The threats of social networking: Old wine in new bottles? *Information Security Technical Report*, *16*(2), 38–43. http://doi.org/10.1016/j.istr.2011.09.008

Yan, G., Chen, G., Eidenbenz, S., & Li, N. (2011). Malware Propagation in Online Social Networks: Nature, Dynamics, and Defense Implications. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 196–206). New York, NY, USA: ACM. http://doi.org/10.1145/1966913.1966939

Yates, I. I. (2010). Practical investigations of digital forensics tools for mobile devices. In *2010 Information Security Curriculum Development Conference* (pp. 156–162). ACM.

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, *3*(3), 17–31. http://doi.org/10.5121/ijcsit.2011.3302

Zainudin, N. M., Merabti, M., & Llewellyn-Jones, D. (2010). A digital forensic investigation model for online social networking. In *Proceedings of the 11th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting, Liverpool* (pp. 21–22).

BIODATA OF STUDENT

Farhood Norouzizadeh Dezfouli is a research student, and is currently studying a Master of Science (Security in Computing) with the Universiti Putra Malaysia. Farhood graduated from the Asia Pacific University College of Technology & Innovation in 2011 with the degree of Bachelor of Science (Information Technology). He was awarded the Silver Medal for the invention/innovation of "Investigating Phishing Attacks" in Pameran Rekacipta, Penyelidikan Dan Inovasi Malaysia 2012. Farhood was also awarded the Certified Ethical Hacker (CEH) and Computer Hacking Forensic Investigator (CHFI) certificates from EC-Council in 2013.