VISUALIZING THUMB DRIVE INFORMATION

FATHIN NAZEERA BINTI MOHD NAZRI

UNIVERSITI TEKNOLOGI MALAYSIA

VISUALIZING THUMB DRIVE INFORMATION

FATHIN NAZEERA BINTI MOHD NAZRI

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JANUARY 2014

“To my Beloved Big Happy Family and Wonderful Best- Friends”

ACKNOWLEDGMENT

Bismillahiramanirahim. Alhamdulillah, thank you Allah s.w.t for giving me the strength to finally finish my study. I would like to express my heartfelt gratitude to my supervisor, Dr. Ismail Fauzi Bin Isnin for his constant support, advices and guidance. Without his encouragement and patience this research would not have been the same as presented here. Not to forget, thanks to all the lecturers for the advice.

I also want to thank my friends for their encouragement and help during my time here in UTM. They are with me when I am in need; they are my true friend indeed. Not forgetting my gratitude to Universiti Teknologi Malaysia and all its staff members for providing me with a comfortable environment and facilities to complete my study. Thank you very much Malaysia Government for sponsoring my Master study.

Last but not least, a deepest love to my beloved family for the courage and endless prayers for me. To Ayah and Mama, thanks for encourage me to continue my study. To my siblings and in-law, Tuty Irma, Zairul Aizec, Amir Azfar, Amir Ahmadi, Amir Asyraf and Nadia Ayuni thanks for always support and give good advices for me. My nephews and niece, Adam, Aidan and Sara, thanks for cheering your aunty.

May Allah bless all of you.

ABSTRACT

Thumb drive is one of portable memory storage that widely used by people. It is popularly used because of the size. It is small in physical size, hence it easy to bring anywhere. Beside the usage of thumb drive bring benefits to the computer user, it also may be used to do crime or as a medium to do the crimes such as used to steal private and confidential data and spread the virus in targeted computer. Luckily, Windows operating system stores all the information of the thumb drive that had been connected to the machine. The information is stored in Windows Registry. Windows Registry in a Windows operating system act as a database of a machine that stores all the system configuration, hardware and software used in that computer, users of the computer, and information regarding the current user of the computer. Thus, the digital crime investigator and security analyst may identify the thumb drive that use to do the crime based on information available in the Windows Registry. This research examined on the type of thumb drive information stored in Windows Registry. A visualization technique was proposed which helps the investigator to search thumb drive information directly from Windows Explorer without using the Registry Editor tool to search the information. It may help them to cut the time of searching the information. Then, the user satisfaction on using the technique was measured by conducting a testing and evaluation session. Two security analysts were appointed to testing and evaluate the user's satisfaction by answering questionnaire at the end of the session. The collected data from the technique and evaluation phase are then analyzed. As the result, the respondents satisfied with the technique by giving average score 3.9 for format element, 4.5 for ease of use, and 4.75 out of 5 marks for both timeliness and satisfaction with the proposed technique speed.

ABSTRAK

Pemacu pena adalah satu daripada simpanan memori mudah bawa yang telah digunakan secara meluas oleh manusia. Ianya kerap digunakan kerana saiznya. yang kecil menyebabkan ia mudah untuk dibawa ke mana sahaja. Penggunaan pemacu pena memberi manfaat kepada pengguna, walaubagaimanapun, ia juga boleh digunakan untuk melakukan jenayah atau sebagai medium untuk menjalankan aktiviti jenayah seperti menjadi alat untuk mencuri data rahsia dan sulit, dan menyebarkan virus ke komputer sasaran. Mujurlah kerana sistem pengoperasian Windows dapat menyimpan semua maklumat mengenai pemacu pena yang pernah dihubungkan kepada sesebuah mesin di dalam Window Registry dimana ianya merupakan pangkalan data yang menyimpan semua konfigurasi sistem, perkakas dan perisian yang digunakan oleh komputer tersebut, pengguna komputer dan maklumat berkaitan pengguna terkini sesebuah komputer. Oleh itu, penyiasat jenayah digital dan penganalisa keselamatan komputer akan dapat mengenal pasti pemacu pena yang telah digunakan untuk melakukan jenayah tersebut berdasarkan maklumat yang tersedia di dalam Window Registry itu. Kajian ini dijalankan untuk mengenalpasti maklumat pemacu pena yang tersimpan dalam Window Registry. Kemudian, satu teknik visualisasi maklumat pemacu pena telah dicadangkan dimana teknik tersebut dapat membantu penyiasat sewaktu mencari maklumat tersebut terus dari Windows Explorer tanpa menggunakan perisian Registry Editor. Teknik ini juga memendekkan masa pencarian maklumat. Seterusnya, kadar kepuasan menggunakan teknik yang dicadangkan diukur dengan melantik dua orang penganalisa keselamatan komputer dengan menjawap satu set soalan berkaitan kepuasan mereka selepas menguji teknik tersebut. Hasilnya, kedua-dua responden berpuashati dengan teknik yang dicadangkan dengan memberi skor purata 3.9 untuk format yang digunakan, 4.5 skor purata untuk mudah untuk digunakan, dan 4.75 skor purata daripada skor 5 untuk masa dan kepantasan menggunakan teknik tersebut.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATION

CD	Compact Discs
CD-ROM	Compact Disc Read-Only Memory
EEPROM	Electrically-Erasable Programmable Read-Only Memory
EUC	End-user computing
EUCS	End-user computing satisfaction
HCI	Human-Computer Interaction
HKCC	HKEY CURRENT CONFIG
HKCR	HKEY CLASSES ROOT
HKCU	HKEY CURRENT USER
HKEY	Handle to a Key
HKLM	HKEY LOCAL MACHINE
HKU	HKEY USERS
ID	Identity
IS	Information system
LED	Light Emitting Diode
MAC	Media Access Control
NAND	Not-AND
NSE	Shell Namespace Extensions
OS	Operating System
PC	Personal Computer
PCB	Printed Circuit Board
PnP	Plug and Play
R1	Respondent 1
R2	Respondent 2
RAM	Random Access Memory
RISC	Reduced Instruction Set Computing

ROM	Read Only Memory
TV	Television
UI	User Interface
URL	Universal Resource Locator
USB	Universal Serial Bus
www	World Wide Web

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

In this modern world, the usage of modern technologies plays huge role in our daily lives, both for work and play. Computers machine whether it is a personal computer, laptop or tablet, as a lifestyle nowadays. Most of Malaysians has at least one of it whether at their home for leisure and entertainment use or at their work place to do their job. Computers make our life easier. With the advancement of internet, the world arguably in our finger tips. We can find millions of information, doing online shopping, watching movies, playing music ant others through the internet.

Computer manufacturers competing with each other sell their best and latest technologies to the customers. The advancement of the computer technology gives variety of choices to the customer to choose whatever the specification that fit their needs and usage such as for gaming purpose, computer as workstation, just leisure usage and others. The important of computer in daily lives may lead the computer architecture design variety of computer accessories such as portable memory storage, audio output devices such as headphone and earphone, variety of printers and such. Portable memory storage such as external hard disc and thumb drives for example become the common devices that computer user has it. The device gives benefit to the users to bring only data or information that they need to anywhere without carrying the laptops. The amount of data stored in that portable memory depends on the size of the devices.

The variety of data and information stored in a portable memory may lead to a computer crime. Webopedia (2013) define computer crime or cybercrime is where any crime in which computer-related technology is encountered. The physical size of portable memory especially thumb drives give benefit to the criminals also known as hackers to use it to steal confidential and private data from the victim. However, most of the computer user did not noticed that every time a new devices connected to a Windows based machine, the devices left their signature in Windows registry (Harlan, 2007). That information gives the cybercrime investigator lead to the digital evidences to identify the offenders.

1.2 Problem Background

Thumb drive also known as pen drive or Universal Serial Bus (USB) drives as a storage devices that have same purposes with floppy disk or CD-ROM which are store data, back up data or transferring data from one devices to others. It is usually small in physical size and it a removable devices. Thumb drives using USB interface to connect the computer system. All the devices such as computer and tablets that have the USB interface can connect with thumb drives.

In forensic investigation, thumb drives can be used as digital evidences because it may contain or store various types of data and information that can lead to the criminals and the crime that they had done. The thumbs drives may be used to store the steal information, alteration of sensitive information, and also can be used to spreading computer viruses and worms. The information regarding thumb drives may help the forensic investigator as a lead to solve crime cases especially in digital crime cases (Bennie, 2005).

A technique regarding on how the investigators to know what thumb drives had been connected to a machine can ease them to search for evidences will proposed. Currently, they have to search manually the information regarding the

thumb drives such as vendor Identity (ID), product ID, Revision and serial number for each device at the windows registry (Khawla, 2010). The proposed technique will visualize all those information related to the thumb drives that had been connected to the Windows operating system.

1.3 Problem Statement

In forensic investigation, thumb drives can be used as digital evidences because it may contain or store various types of data and information that can lead to the criminals and the crime that they had done. The thumbs drives may be used to store the steal information and also can be used to spreading computer viruses and worms. Many crime cases had been solved by having the thumb drives as the digital evidence. Currently, the investigators have to search the thumb drives information in the windows registry. The information related to the thumb drives in the registry may scattered and they have to read all the entries in the registry to search to that information. It may take some times for searching the information.

1.4 Project Aim

The aim of this project is to propose a technique to visualizing the information from windows registry regarding thumb drives that had been connected to computer machine. The user satisfaction on using the proposed technique will be measured at the end of this research work. In the meantime, this project can help the investigator to solve the digital crime by ease them finding such information that can be used as a lead to other digital evidences.

1.5 Project Objective

The objectives of this project have been identified in order to complete this research. There are:

i. To study and identify information related to thumb drives from Windows registry
ii. To design a visualization technique of thumb drive information.
iii. To measure the correctness of the visualization technique and the user satisfaction of using visualization information of the thumb drive.

1.6 Project Scope

In order to complete this project, a number of scopes have been identified and determined, which are:

i. The technique is designed for visualization of thumb drive information from the windows registry.
ii. The technique is for searching information related to thumb drives that have been connected to a machine.
iii. The visualization of the thumb drives will be done on Windows based machine.

1.7 Significance of Project

This project is prepared to produce a technique which can search and visualized thumb drives information in registry. Thus, this project is important to the digital crime investigators to identify the information regarding thumb drives that had been connected to a Windows based computer machine since that information can be

used to them as a lead to other possible digital evidences. They did not have to search that information from each hives and keys in registry because this project may ease them to find it by visualized the information of thumb drives.

1.8 Project Organization

The organization of the project is illustrated as Figure 1.1 below. This project consists of six chapters. The chapters included in this project are introduction chapter, literature review chapter, research methodology chapter, design and implementation chapter, findings and discussion chapter and last but not least conclusion and future works chapter.

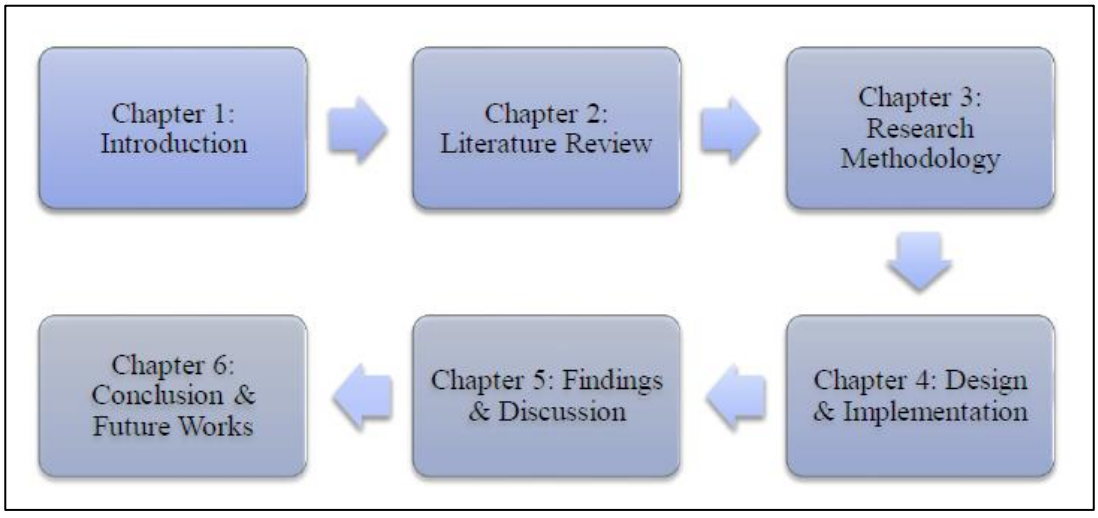

Figure 1.1: Project Organization

Chapter 1 is the introduction has discussed about the background of the problem of this research. Introduction also includes the problem statement, purpose, scopes and objectives to be achieved. The next chapter is literature review. In literature review, the background information of the study is provided. Also detailed information of previous related works which reside on the same domain of this

research is discussed. Chapter 3 is research methodology. Research methodology will discussed phases and process of developing this research. Chapter 4, the design and implementation will highlight the development of the technique. Chapter 5 will discuss the obtain results for analysis and finally, chapter 6 will explain about future works recommendation and conclusion of this research.

REFFERENCES

Bailey, J.E. and Pearson, S.W. (1983) .Development of a Tool for Measuring and Analyzing Computer User Satisfaction, *Management Science*, 29(5), 530-545.

Baroudi, J. J., Olson, M. H. and Ives, B. (1986). An Empirical Study of the Impact of User Involvement on System Usage and Information Satisfaction,. *Communications of the ACM,* 29(3), 232-238.

Bennie, N. (2005). *Forensic Analysis of a USB Flash Drive.* Canberra: SANS Institute.

Benson, D.H. (1983).A Field Study of End-User Computing: Findings and Issues. *MIS Quarterly,* 7(4), 35-45.

Card, S. K., Thomas, P. M., and Allen, N. (1980). The Keystroke-level Model for User Performance Time with Interactive Systems. *Communications of the ACM*, 23(7), 396–410.

Chin, W. W. and Lee, M. K. O. (2000). A Proposed Model and Measurement Instrument for the Formation of IS Satisfaction: The Case of End-User Computing Satisfaction. *Proceedings of the Twenty-First International Conference on Information Systems.* 10-13 December. Brisbane, Australia, 553-563

Doll, W. J. and Torkzadeh, G. (1988). The Measurement of End-User Computing Satisfaction. *MIS Quarterly,* 12(2), 259-274. Accessed from http://www.jstor.org/stable/248851

Doll, W. J., Xia, W. and Torkzadeh, G. (1994). A Confirmatory Factor Analysis of the End-User Computing Satisfaction Instrument. *MIS Quarterly*, 18(4), 453-461. Accessed from http://www.jstor.org/stable/249524

Dunn, M. (2006). *The Complete Idiot's Guide to Writing Shell Extensions - Part I.* from http://www.codeproject.com/Articles/441/The-Complete-Idiot-s-Guide-to-Writing-Shell-Extens. Visited 20/11/2013

Harlan, C. (2007). *Windows Forensic Analysis DVD Toolkit*. Burlington, MA: Syngress Publishing, Inc.

Harsh, B.,Uday, R., and Umesh, S. (2013). *Operating System.* K. J. Somaiya Institute of Engineering and Information Technology

Ives, B., Olson, M. H. and Baroudi, J. J. (1983). The Measurement of User Information Satisfaction. *Communications of the ACM,* 26(10), 785-793. Accessed from http://archive.nyu.edu/bitstream/2451/14594/1/IS-82-27.pdf

Khanse, A. (2011). *Where are the Windows registry files located in Windows 7 | 8.* From http://www.thewindowsclub.com/where-are-the-windows-registry-files-located-in-windows-7. Visited 29/11/2013

Khawla, A. A., Jones, A., and Martin, T. A. (2010). Forensic Analysis of the Windows 7 Registry. *Proceedings of the 8th Australian Digital Forensics Conference.* 30th September. Edith Cowan University, Pert Western Australia

Lin, I. L., Woo, T. K., Chen, Y. C., Lu, T. L., and Shu, I. S. (2012). Study on Constructing Forensics Mechanism of Digital Evidence Based on Information Security Governance Using Digital Evidence Forensic System as an Example. *The International Journal of Forensic Computer Science.* Vol 2, 33 – 45

Nataliya, B. S. (2004). Hacking and Cybercrime. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development.* ACM New York, NY, 128 - 132

Pleas, K. (1996). *Hacking the Registry.* Fawcette Technical Publications.

Russinovich, M. (1999). Inside the Registry. Retrieved 20/11/2013 from http://technet.microsoft.com/en-in/library/cc750583(en-us).aspx

Softpedia, "*Windows 8 Becomes the Fourth Most Popular OS in the World*" http://news.softpedia.com/news/Windows-8-Becomes-the-Fourth-Most-Popular-OS-in-the-World-349853.shtml. Access on 10/11/2013

Tanushree, R., and Aruna, J. (2012). Windows Registry Forensics: An Imperative Step in Trackig Data Theft via USB Devices. *International Journal of Computer Science and Information Technologies.* Vol 3(3), 4427-4433.

The American Heritage Science Dictionary (2005) by Houghton Mifflin Company. Published by Houghton Mifflin Company.

Transcend Information, Inc (2011). *Product Category Rules (PCR) for Preparing an Environmental Product Declaration (EPD) for USB Flash Drive.*

Viksoe, B. (2009). Windows Registry Shell Extension. Via http://www.viksoe.dk visited 1/12/2013

Webopedia, *"Cyber Crime"* http://www.webopedia.com/TERM/C/cyber_crime.html visited 20/9/2013

Wikipedia, *"Data Storage Device"* http://en.wikipedia.org/wiki/Data_storage_device visited 30/9/2013

Wikipedia, "*Digital Evidence"* http://en.wikipedia.org/wiki/Digital_evidence visited 30/9/2013

Wikipedia, *"Digital Forensic"* http://en.wikipedia.org/wiki/Digital_forensics visited 28/9/2013

Wikipedia, "*Human-computer Interaction*" http://en.wikipedia.org/wiki/Human-computer_interaction. Visited 29/12/2012

Wikipedia, *"USB Flash Drive"* http://en.wikipedia.org/wiki/USB_flash_drive visited 25/9/2013

Wikipedia, *"Windows 7"* http://en.wikipedia.org/wiki/Windows_7 visited 30/9/2013

Windows Dev Center, *"IShellFolder::CreateViewObject Method". http://msdn.microsoft.com/en-us/library/windows/desktop/ bb775064(v=vs.85).* visited 23/11/2013

Windows7 (2009). *Welcome to Windows 7*. Microsoft Corporation.

Xiao, Li, and Dasgupta, S. (2002). Measurement of User Satisfaction with Web-based Information Systems: An Empirical Study. *Eighth Americas Conference on Information Systems*. December 2002. 1149-1155

Xie, H., Jiang, K., Yuan, X., and Zeng, H. (2012). Forensic Analysis of Windows Registry Against Intrusion. *International Journal of Network Security & Its Applications (IJNSA).* Vol. 4(2), 121 – 134