A MODEL FORVALIDATION AND VERIFICATION OF DISK IMAGING IN COMPUTER FORENSIC INVESTIGATION

P.SIVA SHAMALA PALANIAPPAN

UNIVERSITI TEKNOLOGI MALAYSIA

A MODEL FOR VALIDATION AND VERIFICATION OF DISK IMAGING IN COMPUTER FORENSIC INVESTIGATION

P.SIVA SHAMALA PALANIAPPAN

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

Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

OCTOBER 2009

Dedicated to my beloved parents,

my respectful brother-in-law and siblings,

my lovely cousins, Pranav and Kailash,

my helpful friends Batch 9, feresa and shazana

With thanks for all the

years of caring, love and support.

ACKNOWLEDGEMENT

In preparing this valuable piece of work, I received much excellent encouragement, guidance and advice from many people surrounding me. These people certainly have contributed towards my success in achieving this piece of work. First of all, I would like to take this opportunity to express my highest appreciation and deepest gratitude to Prof Dr. Azizah Abdul Manaf as my thesis supervisor for giving me full support and faithfulness in all guidance and the necessary support needed for success. I would also like to present my special thanks to my programme coordinator, Dr. Rabiah Ahmad and all my lecturers in CASE. Without their advice, motivation and support, this thesis would not have been the same as presented herein. I thank to all my friends for their support and encouragement.

I also wish to express my sincere appreciation to my parents, brother-in-law, sister and brother who have always encourage and given me full support in doing this project. My sincere appreciation also extends to all computer forensic practitioners' in Malaysia who has provided full support to complete this project successfully.

ABSTRACT

In digital forensic investigation practices, there are numerous digital forensics preservation tools that have been used by practitioners all over the world. Tool development continues as the practitioner’s demands increases. It is important to have right specialized tools in order to ensure that all the collected evidence is processed correctly, completely and in a timely manner, computer forensic practitioners have to employ consistent and well-defined forensic guidelines to validate and verify the computer forensic tools. Moreover, guideline of validation and verification in computer forensic tools provides a great opportunity for computer forensic practitioners to remove necessity for developing individual tests for tools. Since computer forensic practitioners’ in Malaysia are not aware of the significant of validation and verification of disk imaging and there is no standard guideline for disk imaging process, thus a guideline model for validation and verification for disk imaging has been created. A qualitative research method was adopted as a research strategic methodology to examine and review the level of acceptance towards proposed guideline for validation and verification of disk imaging. Thirty seven respondents participated in the survey as the questionnaires are only targeted at the forensic experts in Malaysia. The survey result has shown majority of the respondents do agree with the proposed guideline. The survey results provide indication on the process of developing guideline of validation and verification of disk imaging in Malaysia and manage to produce a new conceptual model to validate and verify the disk imaging tools in computer forensic environment. This conceptual model is emphases more on the management element which encompasses three supporting elements that are documentation, maintenance of tools and monitoring. The internal layer are consists of technical elements which are divided into checklist of mandatory features, checklist of optional features and report writing.

ABSTRAK

Dalam proses penyiasatan digital forensik, terdapat pelbagai jenis alat penyalinan forensik digunakan oleh para pegawai forensik yang mahir dalam bidang ini. Proses pembangunan alat-alat forensik berterusan selaras dengan permintaan yang meningkat dari pegawai forensik. Pegawai komputer forensik perlu memastikan alat penyalinan yang betul digunakan untuk memastikan segala bukti yang dikumpulkan adalah betul, sepenuhnya dan menepati masa yang diperuntukan. Bagi memenuhi permintaan alat alat forensik , pegawai komputer forensik perlu menggunakan panduan bertulis yang konsisten dan teratur dalam proses pengesahan dan kesahihan alat penyalinan tersebut. Tambahan pula, panduan pengesahan dapat meringankan beban pegawai forensik untuk membina ujian individual bagi setiap alat penyalinan yang hendak digunakan. Pegawai forensik di Malaysia tidak menyedari ketidakwujudan panduan bagi proses pengesahan alat penyalinan. Sebagai langkah cadangan, projek ini dikendalikan untuk menghasilkan panduan bagi proses pengesahan alat penyalinan bagi pegawai-pegawai forensik di Malaysia. Kajian jenis kuantitatif telah digunakan untuk menyelidik and mengulas tahap penerimaan pegawai forensik Malaysia terhadap panduan pengesahan alat penyalinan yang dicadangkan. Seramai tiga puluh tujuh responden yang mahir dalam bidang forensik telah mengambil bahagian dalam kajian ini dan majoriti telah bersetuju dengan cadangan panduan pengesahan untuk alat penyalinan. Hasil kajian ini menjuruskan ke arah penyediaan panduan pengesahan bagi alat penyalinan dan juga konseptual model yang menerangkan elemen-elemen yang terlibat dalam proses pengesahan alat penyalinan. Terdapat dua bahagian di mana bahagian luar dikenali sebagai sokongan yang terdiri daripada dokumentasi, penyelengaraan alat dan pemantauan. Manakala bahagian dalam terdiri daripada elemen-elemen teknikal yang berkaitan dengan proses pengesahan alat penyalinan.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

With the development of modern computers and networks, computer-related crimes has become a threat to society because of the immense damage it can inflict while at the same time it has reached a level of sophistication which makes it difficult to track it to its source. However, any computer crime leaves a trail of evidence in the form of digital information stored or transmitted on electronic components. In order to be usable as evidence in a court of law, such information needs to be captured in a systematic way without altering it in so doing. Due to the application of computer technology used to investigate computer-based crimes, a new specialized field called forensic computing has been developed, becoming famous worldwide amongst the digital crime scene.

There have been many attempts to define the computer forensics. Forensic is defined as belonging to, used in, or suitable to courts of judicature or to public discussion and debate (Bologna and Lindquist, 1995). Computer forensics is the coherent application of methodical investigatory techniques to solve crime cases (Kruse and Heiser, 2001). McKemmish (1999) an Australian practitioner in the field, postulates the four main concepts of identification, preservation, analysis and presentation, which has been prevalent in the field and often cited.

Brian Carrier (2003) attempts an all-encompassing definition, “The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”

In the digital forensics investigation practices, there are over hundreds of digital forensics tools that have been used by practitioners all over the world. Tool development continues as the practitioner’s demands increases. Kruse and Heiser (2001), points out those new tools provide approaches to automated examination and analysis. Different types of application will need different types of tools to preserve and analyze the evidence. However, choosing the appropriate tools to a crime case situation will save time in the police investigation cases.

Thus, it is important to have the right specialized tools in order to ensure that all of the collected evidence is processed correctly, completely and in a timely manner. This is because there are five rules to consider when collecting evidence by using tools. One, is the evidence admissible, or usable in court? Two, is the evidence authenticate, or does it relate to the incident? Three, is the evidence complete? Four, is the evidence reliable? Five, is the evidence believable? Researchers, investigators, legislators and jurists are all advised to use proven investigative techniques and methods exist in the traditional forensic disciplines. To catch and prosecute criminals involved with digital crime, investigators must employ consistent and well-defined forensic procedures (Silverstone and Davia, 2005).

Providing accurate information derived through the use of proven and well-understood methodologies has always been the goal of traditional forensic analysis. Forensic Science applied in court of law has sought to use commonly applied techniques and tools only after rigorous, repetitive testing and through scientific analysis.

1.2 Background of the Problem

Today’s global world is increasingly reliant on digital sources of information and the computerized systems and networks involved in data storage, processing, and transmission. This growing reliance drives development to advance required technology. The criminals, terrorists, and other nefarious members of society have not neglected these facts. Thus words like cybercrime, cyberwar and cyberterror have started to become more ordinary nowadays.

Due to rapid technological attacks, investigators are facing difficulty in applying currently available preservation tools because the tools sophistically are changing. Currently, there are a lot of unknown trust levels of tools in development in computer forensic environments. It is essential that research steeped in the scientific method becomes fundamental to discovery and enhancement of all tools and technologies employed to assist the courts, including digital forensic evidence (Palmer, 2001).

Forensic computing has typically developed out of a demand for services from the law enforcement community (Noblett, Pollitt and Presley, 2000) and typically developed in an ad hoc manner (Etter, 2001) rather than a scientific one. According to Jason and Jill (2007) many forensic computing practitioners are working in a high workload and low resources environment are finding difficulty in meeting demand of validation and verification of their tools and still meet demands of the accreditation framework.

It seems many agencies cannot verify the results with their equipment and mostly rely only on an independent validation study of other peoples’ equipment; it raises issue of tools in reality never being tested. Jason and Dr.Jill (2007) also identify that independent tools is expensive and time consuming. Apart from that, many practitioners are using tools which were not originally designed for forensic purpose. In a dynamic work environment, the evidence changes at such an exponential rate that forensic tools are modified regularly with the intention of to keep up. In addition, the issue regarding the validation and verification is diversity of tools. This is because variety types of tools will cause the computer forensic practitioners facing problem to develop validation and verification guideline for each tools. It is difficult to have an individual tool to meet all requirements in the investigation. There will be different types of tools for each forensic investigation.

There are a number of frameworks and guidelines developed from authorized bodies, such as the Department of Justice and the Association of Chief Police Officers in the UK. But none of these models specifically discusses the validation of tools and processes (Jason and Jill, 2007). When there is no standard, the review of experts in the field and any other authorized parties is required.

Giordano and Maciag (2002) pointed out some of the current cyber forensic challenges:

a. There are no universal processes or scientific underpinnings in the methods used to recover or interpret digital information. Even there are varied processes and techniques available in forensic investigation, there are no metrics established processes or best practices that are in use.
b. There is a lack of standards to guide or derive commercial or military development of digital forensic tools and technology (National Institute of Justice, 2002). Academia and enforcement have built ad hoc tools for cyber forensic purposes nevertheless the vendors have built propriety forensic tools that require expensive support.
c. There is a lack of adequate community information sharing for developed tools and technologies.

It can be concluded that as digital forensics has come of age, the issue of appropriate standards or best practices in validation and verification of forensic tools is lacking. Proper standard will hasten the time from development to approval for forensic computing tools.

1.3 Problem Statement

It is detected there is no research has been conducted for validation and verification in computer forensics tool (disk imaging) in Malaysia. It is possible that this issue is not realized by the Malaysian investigators and it is essential to find a solution for this problem. The problems statements that lead to this topic are as below:

1. Not aware of the significant of validation and verification of computer forensic tool (disk imaging);
2. No standard guideline in the validation and verification for disk imaging process due to sophisticated nature of tools and crime committed.

1.4 Project Objectives

The objectives of this study will be as follows:

1. To investigate the availability of validation and verification process for disk imaging in computer forensic tools;
2. To study the available standards which comply to the purpose of validation and verification model for disk imaging;
3. To develop conceptual model and guideline model for validation and verification in digital forensic tool for disk imaging; and
4. To validate and analyze the proposed guideline of validation and verification in computer forensic tool for disk imaging.

1.5 Project Aim

The aim of this study is to propose a conceptual model for validation and verification in disk imaging in computer forensic.

1.6 Project Scope

The scope for this study covers the validation and verification in disk imaging at Polis Di Raja Malaysia and develop guideline model to validate and verify the Disk Imaging process in a computer forensic tool. The questionnaires will be distributed to computer forensic practitioners at Malaysia.

1.7 Summary

The gains of international bodies linking researchers and practitioners not only builds the structure of the digital forensics discipline but also allows that if the validation process already undertaken overseas can be verified, then the result can be accepted within Malaysia.

The introduction of guideline model into modern digital forensic laboratories has many implications to practitioners in the discipline. The validation and verification in computer forensic tools will enable testing to be conducted promptly and if required, there is applicable guideline model in computer forensics for reference and guidelines.

Validation and verification in computer forensic tool provides great opportunity for Polis Di Raja Malaysia to remove necessity for developing individual tests for tools. The guideline model will provide a basic guideline for the digital forensics disciplines to adapt for its requirements. It seems that many tools are not developed specifically for the purposes of digital forensics and hence forth, the guideline model in validation and verification will definitely help the police to conduct the investigation and in their daily work.