# GUIDELINE FOR FORENSIC ANALYSIS
# ON WINDOWS XP AND VISTA REGISTRY

**SOMAYEH AGHANVESI**

**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 Computer Science and Information Systems**
**Universiti Teknologi Malaysia**

**OCTOBER 2008**

# ABSTRACT

On the age of digitalization world and dependencies of people to digital system having a schedule to protect their assets is obvious. Digital hacking is always one of hot subject in information security field. So many organizations need special training to be covered and protected against hackers. Also like every crime which is being investigated the hacking and digital crimes also are being surveyed and the related evidences are being collected through digital investigators who are forensic specialist. Forensic is a science to collect the evidence against hackers in digital world.

The Focused issue on this project is collecting the evidences from a limited scope of Microsoft windows Vista and XP versions which is their Registry platform which is one the areas that has valuable information but is not being considered by specialist as well as other areas because of its complexity. The registry platform is the place windows stores all the configurations and this place potentially have evidences inside which need to be found in sake of forensic examination.

The number of keys is a lot and searching the keys by each investigator is a tedious work. The keys need to be searched, analyzed, evaluated from forensic value, be considered in evidence management process and being sorted in a referable manner for investigators. That is why we decided to prepare a guideline for investigators interested to have a look to the evidentiary keys and their values. Also as second part of this guideline we have prepared the investigation steps on registry area with Encase tool which is chosen among many tools available currently and have been surveyed so far.

# ABSTRAK

Perlindungan aset di dalam dunia digital kini adalah sangat jelas dan kebergantungan kepada sistem digital juga sangat tinggi. Pencerobohan digital kerap berlaku di dalam keselamatan maklumat. Banyak organisasi memerlukan latihan khas bagi melindungi aset mereka daripada penceroboh., Semua bukti digital yang berkaitan pencerobohan dikumpulkan oleh pakar forensik bagi setiap kes yang disiasat. Forensik merupakan sains dalam mengumpulkan bukti bagi menentang pencerobohan di dalam dunia digital.

Isu yang difokuskan di dalam projek ini adalah berkaitan dengan pengumpulan bukti bagi sistem pengoperasian versi Microsoft Windows Vista and XP di mana platform *registry* yang merupakan salah satu punca maklumat yang sangat berharga tetapi tidak dipertimbangkan oleh pakar disebabkan oleh cirinya yang sangat kompleks. Platform *registry* adalah tempat di mana Windows menyimpan semua konfigurasi yang berpotensi untuk menjadi bukti yang perlu ditemui bagi setiap insiden pencerobohan.

Mencari *key* oleh setiap penyiasat forensik adalah sangat rumit kerana jumlah *key* berkenaan adalah terlalu banyak. *Key* berkenaan perlu di cari, di analisis dan di taksir dari aspek forensik yang kemudiannya akan di pertimbangkan di dalam proses pengurusan bukti. Oleh yang demikian, projek ini bertujuan untuk menyediakan garispanduan bagi penyiasat forensik dalam menaksir setiap nilai bukti. Dan sebagai bahagian kedua garispanduan ini, disediakan juga langkah-langkah bagi memulakan siasatan bagi *registry* dengan menggunakan peralatan yang ada pada masa kini iaitu *Encase*.

# TABLE OF CONTENTS

# Chapter 1

# Introduction

## 1.1 Preamble

In the world the using of the Digital systems and people dependencies are getting more, and also the breaches and thefts as well as technology features are growing up and the assets needs to be maintained secure more than before, thus the information assets are becoming more critical. The digital forensic investigation is the way to get penetration's track and find the evidences on this field, and investigation on windows registry is one of these issues that needs to be considered more than before.

The introduction of this study will start with basic definition of investigation on windows XP and Vista which will be explained on further pages with the expression of "Registry", "Forensic", "Evidence", "Investigator" and "Hacker" definitions.

Windows Vista and Windows XP store configuration data in registry. It is a central repository for configuration data that is stored in a hierarchical manner. System, users, applications and hardware in Windows make use of the registry to store their configuration and it is constantly accessed for reference during their operation. The registry is introduced to replace most text-based configuration files used in previous Windows versions, such as .ini files, autoexec.bat and config.sys. Due to the vast amount of information stored in Windows registry, the registry can be an excellent source for potential evidential data. For instance, windows registry contains information on user accounts, typed URLs, network shared, and Run command history.

The Registry is a large, complicated database (about which we can find tons of material on the web).The Registry consists of thousands of individual entries. Each entry consists of two parts, a key and a value. Each value is the setting for its associated key. The Registry organizes the entries into hierarchies.

To make the scope of this study more clear here is the definition of main words we have on this project:

**Computer forensics**, Forensic is the art and science of applying computer science to aid the legal process. Although plenty of science is attributable to computer forensics, most successful investigators possess a nose for investigations and for solving puzzles, which is where the art comes in.

**Evidence** in its broadest sense includes anything that is used to determine or demonstrate the truth of an assertion. Philosophically, evidence can include propositions which are presumed to be true used in support of other propositions that are presumed to be falsifiable. The term has specialized meanings when used with respect to specific fields, such as policy, scientific research, criminal investigations, and legal discourse.

**Investigation** is the process of inquiring into a matter through research, follow-up, study, or formal procedure of discovery. And also is Academic or intellectual investigation aimed at the discovering, interpreting, of knowledge.
Put simply, applied forensic computing comprises four main stages, namely:

- Identifying sources of digital evidence
- Securing and preserving identified evidence
- analyzing the evidence
- documenting legally admissible evidence

**Hacker,** in a security context, a hacker is someone involved in computer security/insecurity, specializing in the discovery of exploits in systems (for exploitation or prevention), or in obtaining or preventing unauthorized access to systems through skills tactics and detailed knowledge.

Thus, it is more than the technological, systematic inspection of the computer system and its contents for evidence or supportive evidence of a civil wrong or a criminal act. Computer forensics requires specialized expertise and tools that goes above and beyond the normal data collection and preservation techniques available to end-users or system support personnel. One definition is analogous to "Electronic Evidentiary Recovery, known also as e-discovery, requires the proper tools and knowledge to meet the Court's criteria, whereas Computer Forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence."

## 1.2 Background of the Problem

Since the usage of PC and Windows operating systems are increasing, the people get used to work and rely more to the automation of systems of digital world; although the threats and warns will become more considerable beside the benefits of digital system usage; so the role of hackers is like getting benefit of the penetration and cheating the systems when investigation role is about analyze and find the latest information from improved, updated and developed systems and protecting rights by present the beyond reasonable doubt evidences to court which is more critical to maintain the systems life.

Through analyzing the registry of the windows Vista and XP, the survey of the limitation of registry platform, advantages, Whys, and Hows, problems, tools will be conducted and we will be able to find out evidences which are worth to present in court and categorized specifically on registry platform. Whereas according to complex environment of registry, the investigation on windows Vista and XP registry field is not as strong as other areas of such operating systems so the deficiencies of a complete secure guideline on registry investigation is obvious. Also beside the experiment in this project some flaws will be derived and proved from Windows registry, to bring challenges and solutions of future work.

With the rise in incidents of unauthorized access, modification or simply the theft of digital assets, none of the organization can afford to ignore information security systems designed to protect such assets so aimed at IT professionals and business executives in corporations, organizations and government agencies as well as lawyers seeking an introduction to this emerging practice area. the Law, Investigation & Ethics specialists seeks to:

- Identify legal risk issues in the design, development and management of information technology (IT) security systems.
- Introduce key legal concepts in the protection and management of digital assets.
- Outline key legal risk management principles and strategies that organizations should adopt as part of their information security policy;
- Provide an overview of investigation processes and techniques when a computer crime is suspected to have been committed; and
- Provide a practical guide in the management of digital evidence to ensure that such evidence meets the legal standards and requirements in court proceedings.

And some risks and exploitations currently can be done by hackers through registry alteration are such as:

- Registry key changes
- System configuration altering
- Making start up changes
- Auto run features
- Error creating
- Data hiding
  - Logging information altering
  - Hidden file execution
  - Virus and Trojan attacks
- Password sniffing by running a code through registry alteration

Therefore, the security issues as listed below must be enforced in inspection schedule of registry forensic investigation guideline, to make sure the process of having investigation is in clear sort in order to provide an easy use and refer forensic guideline:

- Confidentiality to ensure that data stored in registry hives, cannot be read by unauthorized third parties, and to find the third party's attached fingerprints or evidences.
- Integrity to ensure that data stored in registry repository cannot be changed by unauthorized third parties, and to find changed value and it's agent.
- Availability to ensure that data is available to authorized parties and systems and/or programs at all times, and to find the agent has changes permision to unauthorized party.
- Identification and authentication to ensure that the user is properly identified and verified during the log-on process, otherwise to find the reason has granted access to unauthorized party.
- Authorization (logical access control) to ensure that the user only has access to that data hives which is relevant to him/her, and not to other data, otherwise to find the reason has granted access to others.
- Non-repudiation to ensure that a user can be held individually responsible for any action performed on the system.
- Strong firewall usage and firewall logging feature in sake of hardening system attacks.
- System configuration or backup and restoere of reistry on sytem.

The Information security issue identified above should be addressed by ensuring that the registry Information countermeasures are conducted throughout the windows Vista and XP provided investigation guideline.

## 1.3 Problem Statement

During the process of investigation many of investigators need to know how to find evidences against hackers or find indicative information through Windows XP and Vista registry in a clean and compact sort which is drawn attention to this project objective. For the purpose of this project among the problem statement are as follow:

- Since there are prepared investigation software help many investigators to find the evidences on systems, there needs to evaluation between different tools and recommendation of the best tool which is acceptable by legal firms and find out the main key points to investigate the registry through this tool. Then the main need is registry investigation guidelines with this tool in windows XP and Vista environment which is not available currently such special investigation guidelines.

- Some of information can be found by manual investigation of Windows Registry keys and many of investigators or even the normal users do not have the software or a professional tool and they prefer to have manual finding through registry keys. In such case the important data which can be useful for them needs to be collected in a guideline so users can refer straight to collected keys without wasting time and having experience through complex environment of registry platform since the keys and the information will be embedded in guideline will have the test, implement and develop sessions, to find certain information. Some of useful information can be as follow:

    - Websites that suspect has ever visited
    - Outlook emails and deleted information after they delete their Outlook emails and empty the Recycle Bin

- Login information
- The network hacker attached and computer is been connected
- Software might run and act as a spy
- Microsoft Word and Excel documents contain secret keys that uniquely identify suspect
- The hackers IP address connected to this system
- And so on with more information

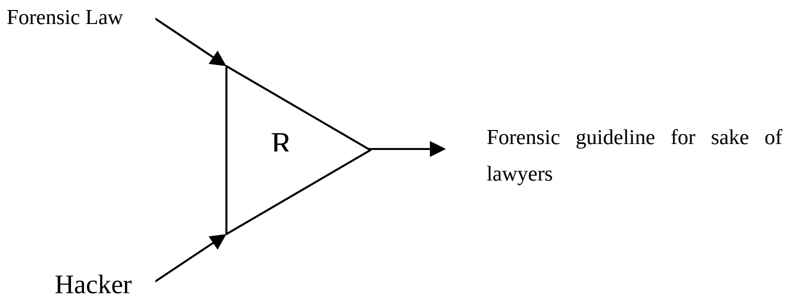

Figure 1.3: Problem Statement

Investigators of windows forensic have to follow all the technical and complicated steps to get the evidences and of course this process will get time and needs some technical skills and tools which need to be attended. For example knowing about SID numbers, LSA secrets, needs to focus on the background knowledge of windows which is not smoothly and fast understandable.

## 1.4 Project Aim

Bringing evidences for windows XP and Vista needs to study all around windows registry scope to get accurate data collect them in a proper sort and make it more understandable for investigators whereas registry part of windows have been always sound difficult or not smooth understandable although in a way it can be useful and informant.

The objectives of doing this project are:

- Analyzing of the registry on windows XP and vista operating systems;
- Categorizing the importance of the registry on information security, and promote the ideas to protect systems against hackers and bring more exact and accurate evidence;
- Help the investigators to collect the information as evidence in the correct and confident way and prepare the evidences.
- Study on the new features added on windows Vista.
- Study the risks which make the windows unstable or unsecure to be hacked by black hats.
- Study and propose a tool and necessity of having it to have reliable investigation on registry area which is acceptable on courts.
- Study the extent of damages on system after they have done.
- Study the system recovery.
- Preventing the systems from future attacks.
- Writing a complete guideline for those who want to have a complete search on registry of windows XP and Vista and pass the skill of digital forensic investigation with one of the high evaluated current tools.

## 1.5 Project Scope

The project scope indicates the areas and limitation on this project in terms of process, coverage, participants and collaborators is as sorted below:

- This project is being performed on the registry of Windows XP and Vista versions.
- The analysis of registry keys in term of finding new evidences against hackers or information which would be useful for investigators.
- Study the Forensic Registry investigation approaches to prove the incident has indeed occured.
- Study the extent of damages can be done by hackers on victims system.
- Study the system recovery approaches after damage has accured.
- Study the approaches to hardening systems from future attacks.
- The analysis of the registry files which store the values in certain system files with certain extensions.
- The analysis and the usefulness of certain keys in forensic field.
- Studying the registry keys would be in limitation of Internal or external Network systems.

# REFERENCES

*1)* Wong, L.W. and E. C. U. (2007). *Forensic Analysis of the Windows Registry*. School of Computer and Information Science.

*2)* Anson, S. Bunting S. (2007). *Mastering Windows Network Forensic and Investigation*. Sybex.

*3)* Mueller, L. and lance mueller. (CEIC 2007). *Basic investigation of Windows Vista.*

*4)* Mueller, L. and lance mueller. (2007). *Fundamental Computer Investigation Guide for Windows.*

*5)* Mark R. and Bryce C. (2006). *RegMon for Windows v7.04*

*6)* *Fundamental Computer Investigation Guide for Windows.* Microsoft proc.

*7)* Derrick J. Farmer. Burlington, Vermont A .*Windows Registry Quick Reference for the Everyday Examiner.*

*8)* Derrick J. *(2007) Forensic analysis window registry.*

9) *Windows Registry FAQ.* a survey. Proc. Microsoft Corp. (http://support.microsoft.com/kb/304590/en-us)

10) *Useful tools for package and deployment issues,* Microsoft corp. http://support.microsoft.com/kb/198038/en-us

11) Salvatore J. and Frank Apap. *A Comparative Evaluation of Two Algorithms for Windows Registry Anomaly Detection.*

12) Matthew G. (2006). *Counter-Forensic Tools: Analysis and Data Recovery.*

13) *Error message in Windows Vista when you use Registry Editor to load a registry hive file that is on a shared network resource cannot load HivePath filename Access is denied_files,* Microsoft Corp. http://support.microsoft.com/kb/936756/en-us

14) *How to set or change registry editing permissions in Windows XP or in Windows Server 2003_files,* Microsoft Corp. http://support.microsoft.com/kb/310426/en-us

15) *Differences between Regedit.exe and Regedt32_files,* Microsoft Corp. http://support.microsoft.com/kb/141377/en-us

16) Mark R. and Bryce C. (2006). *How to Read from the Windows Registry.*

17) Hor Cheong Wai. And Major. (1993). *RESEARCH IN COMPUTER FORENSICS.*

18) John W. (2007). *Knowledge Base FAQ's,* WWW.consumers-reviews.net, www.regcure.com.

*19)* (2005-2006), *Vista compatibility investigation guide*, Microsoft Corp.

*20)* (2007). *Windows registry information for advanced users*, Microsoft Corp. http://support.microsoft.com/kb/256986/en-us.

*21)* Kumar, R. (2005). *Research Methodology: A Step-by-Step Guide For Beginners*. SAGE.

*22)* Mauch, J. and N, Park. (2003). *Guide to the Successful Thesis and Dissertation - A Handbook for Students and Faculty*. USA: Routledge.

*23)* Kothari, C. R. (1990), *Research Methodology: Methods & Techniques. (2th ed.)* New Delhi: Wishwa Prakashan.

*24)* Cobb, M.(2007), *How vulnerable is the Windows registry.* www.searchsecurity.com

*25)* Gralla, P. (2007). *Windows Vista Pocket Reference.* United States of America. O'Reilly Media, Inc. Jepson, B (Ed.).

*26)* Guidance Software. (2004). *NIST Computer Security Incident Handling guide.*

*27)* AMUST Software. (2005).*4 Myths about Windows XP Registry Cleanup.*