

**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

TABLE OF CONTENT

CHAPTER	TITLE	PAGE
	TITLE PAGE	i
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENTS	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xiii
	LIST OF FIGURES	xi
	LIST OF APPENDIXES	xii

DEDICATION

This thesis is dedicated to the first and the last who is Allah though it's too little but reminds me always refer to him because always he give me the bests.

Also this thesis is dedicated to my gentle husband who always supports me and I wish the perfect life for him.

Finally, this thesis is dedicated to all those who believe in the richness of learning.

ACKNOWLEDGMENT

All praise is to Allah, the most Merciful, for His Love and Guidance, Salutations on the Prophet Muhammad (*PBUH*), his family and fellow companions.

May I express my appreciation to ALLAH, the beneficent, the merciful, for blessing me with the privilege of acquiring a higher degree.

AP Dato' Prof. Dr. Norbik Bashah Bin Idris, my supervisor gave me all the necessary support needed for success, as such, I owe it a duty to be appreciative.

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

I	Introduction	1
	1.1 Preamble	2
	1.2 Background of the Problem	5
	1.3 Problem Statement	8
	1.4 Project Aim	9
	1.5 Project Scope	11
	1.6 Project Requirement	12
 II	 Literature Review	 13
	2.1 Introduction	13
	2.2 Windows Registry	14
	2.3 Registry Structure	14
	2.4 Registry History	16
	2.5 Registry Organization and Terminology	17
	2.6 Registry Concepts	19
	2.6.1 Why Registry Must be Written Directly	19
	2.6.2 Making Restore Point on Windows	20
	2.6.2.1 Restore Point Hack	21
	2.7 Forensic Analysis of the Windows Registry	22
	2.7.1 Value	23
	2.8 Registry Root Key Organization	27
	2.8.1HKEY_USER	27
	2.8.2HKEY_CURRENT_USER	28
	2.8.3HKEY_LOCAL_MACHINE	30
	2.8.4HKEY_CLASSES_ROOT	31
	2.8.5HKEY_CURRENT_CONFIG	32
	2.8.6 Registry Hives	32
	2.8.7 Registry Search	34
	2.9 Registry Improvement	35
	2.9.1Registry Improvement on Windows Vista	35
	2.9.1.1 Registry Virtualization on Windows Vista	37
	2.10 Registry Investigation with Forensic Tool	38
	2.10.1 Encase Registry Forensic	38
	2.10.2 Why Choosing Encase	41
	2.10.3 Using Cain to Decrypt the Protected Storage System	42
	2.10.3.1 Disable Most Recently Used (MRU) Files List by Hackers	45

2.11	Manually Information Extraction	45
2.11.1	Finding Information on Software Key	46
2.11.2	Installed Software	47
2.11.3	Last Logon	48
2.11.4	Windows Firewall Logging	49
2.11.5	Exploring Security Identifiers	49
2.11.6	Investing User Activity	52
2.11.7	Registry Last write time	53
2.11.8	The Key value Corresponds Remote Desktop Running	54
2.11.9	The Keys are used for automatic Program Startup	55
2.12	Recover from Corrupted Registry	56
2.13	Registry Protection	56
2.14	Ease of Use or Security	57
2.15	Forensic Value of Registry Keys	59
2.16	LSA Secrets	69
2.17	Finding Clear Text Password in the Swap File	71
2.18	Discovering IP Address	71
III	Research Methodology	73
3.1	Introduction	73
3.2	An analysis of Registry Principles	76
3.3	Study the Individual Methods to Investigation	77
3.4	Techniques for registry Improvement	78
3.5	Investigation Quality Evaluation	78
3.6	Study Evidences for admitting in Court	79
3.7	Study the other Secret areas	79
3.8	Study the Tools	79
3.9	Finding Registry Problems	80
3.10	Test Evidence Accuracy	80
3.11	Writing Structured Guideline	81
IV	Chapter4: Guideline	82
4.1	Introduction	82
4.2	Audience and Assumptions	84
4.3	Experiment of Guideline Production	86
4.4	Implementation Digital Investigate via Encase	87
4.5	Guideline	88
4.5.1	Windows XP and Vista Registry Platform Keys Guideline	88
4.5.2	Windows XP and Vista Registry Forensic Guideline Via Encase Tool	117

V	Discussion	121
	5.1 Introduction	121
	5.2 Performance of Windows XP and Vista Guideline	122
	5.2.1 Influence of Windows XP and Vista Guideline on Defined Users	122
	5.2.2 Guideline Usability Statement between Different Users	123
	5.3 The Literature Review and Conclusion	124
	5.4 Hidden Information in Registry Entries	125
	5.5 Time	126
	5.6 Registry Cleaners	127
VI	Summary and Further Work	130
	6.1 Summary	130
	6.2 Further Work	132
	REFERENCES	133

LIST OF TABLES

FIGURE NO.	TITLE	PAGE
2.5	Registry Value Data Type	17
1.7	Root and Abbreviation	22
2.8.2	HKCU Sub Keys	29
2.8.3	HKEY_LOCAL_MACHINE	30
2.8.6.1	Registry Path – Hive and Supporting Files	33
2.8.6.2	File Extension and Description	34
2.14	Ease of Use of the Security	57

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
1.3	Problem Statement	9
2.3	Registry Structure	15
2.7.1.1	Registry String Value	23
2.7.1.2	Binary Values	25
2.7.1.3	DWORD Values	25
2.10.1	Encase Forensic Tool	39
2.10.3	Protected Storage System (MRU)	43
2.11.1	Software Key	46
2.11.3	Winlogon	48
2.11.5.1	SID Number	50
2.11.5.2	SID Numbers And Profile Image Path	52
2.11.7	Registry Last Write Time	54
2.15	MRU on Registry	61
2.18	IP Addresses And Configuration	72
3.1	Research Methodology Adopted	74
4.1	Guideline Structure	81
5.5.1	Interest of using Regedit.exe	119
5.5.2	Interest of Using Encase	120

LIST OF APPENDIXES

APPENDIX	TITLE	PAGE
A	Registry Keys and their Correspondent information	136

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 permission 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 restore of registry on system.

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

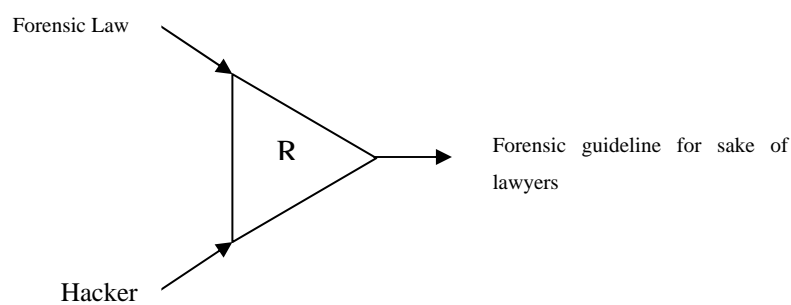


Figure 1.3: Problem Statement

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 occurred.
- 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.

- Find out the important usage of the forensic registry tools such as encase.
- The output of this study would be a guideline in aid of digital forensic investigators.

1.6 Project Requirement

The requirements of this study would be two versions of windows XP and Vista which the study of their Registry keys will be conducted. The tool we will survey to have investigation of registry keys through it will be the Encase Software and later the reason of choosing such tool will be explained. The firewalls, antivirus and the tools can be useful of having secure environment to prevent getting attacked by hackers is another requirement of this project. The files containing registry data inside and have special extension is also considered in this study.

Chapter 2

Literature Review

2.1 Introduction

On this stage we will collect the most important information about registry and most important issues from forensic point of view. So the study is started by definition of registry and basic knowledge about it. Then by continue through the technical study there will be review the valuable keys on registry which have forensic value. All these information needed to have enough experience and knowledge about firstly the registry and then the registry forensic to come out with comprehensive guideline for investigators. The entire subject are being studied are from registry keys, hives, and the ways to collect evidentiary information. So then we will have enough idea to categorize the information and analyze them to bring the sort of investigation forensic guideline.

2.2 Windows Registry

Lih Wern Wong (2006) indicates the Windows Registry contains lots of information that are of potential evidential value or helpful in aiding forensic examiners on other aspects of forensic analysis. Windows XP and Vista 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 Windows 3.x and MS-DOS, such as .ini files, autoexec.bat and config.sys.

Bunting Steve (2007) also indicates Due to the vast amount of information stored in Windows registry; the registry can be an excellent source for potential evidential data. In instance, windows registry contains information on user accounts, typed URLs, network shared, and Run command history. Aspects discussed in this study are based solely on Windows XP and Vista registry.

2.3 Registry Structure

According to Lih Wern Wong (2006) Figure 2.3 shows Windows registry logical view for Register Editor (Windows default register editor). Each folder in the left key pane is a registry key. The right panes show the key's value. Subkey is used to show the relationship between a key and the keys nested below it. Branch refers to a key and all its subkeys.

Windows uses symbolic link (i.e. similar to file system's shortcut) to link a key to a different path which allows the same key and its values to appear at two different paths (Russeinovich, 1999).

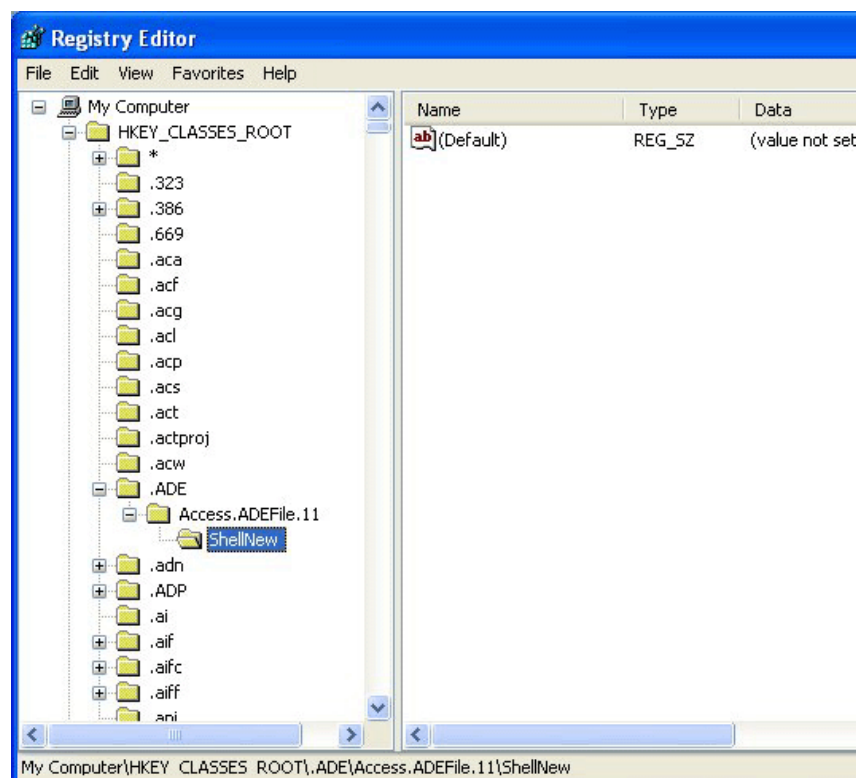


Figure 2.3: Registry Structure

The windows Registry is a vast hierarchical database of operating system, program, and user settings. It's also a relatively obscure Windows feature in which the user rarely has direct interaction. The Windows Registry contains Information that is significant for the investigator conducting network investigations. Accordingly, to access this information and intercept it's meaning, the network investigator must have a good understanding of the windows Registry (Lih Wern Wong 2006).

2.4 Registry History

Before the introduction of the registry, all of this information was stored in literally hundreds of individual .ini (initialization) files. With such an arrangement, there was usually at least one .ini file per program, and they were scattered throughout the file directory. The registry was introduced to create a single repository for system and application configurations (Michael Cobb 2007).

The Microsoft Windows operating system has its roots in MS-DOS was a command-line interface whose configuration setting. MS-DOS received its configuration setting from two small files, config.sys and autoexec.bat. The config.sys file primarily loaded Device drivers, while autoexec.bat was for setting environment variables, running program, and the like (Lih Wern Wong 2006).

The first windows graphical user interface (GUI) was Microsoft windows 3.0. This first version of windows introduced INI files as containers for configuration files. These INI files were flat even so, their length and the amount of data in them made management difficult. Furthermore, it was difficult to store binary data in text files (Derik J, Farmer 2006).

Windows 3.1 followed shortly after windows 3.0, and with it came the rudiment of the system Registry. This system Registry was organized in a hierarchical file system and was used as a repository for system configuration settings. Windows 95 and NT 3.5 expanded the Registry to the structure and interface that we find today in windows XP/2003. Although the structure and interface are similar between the early version and today's version of the registry, its size and complexity have grown tremendously. In

addition, the files in which the registry values are stored have gone from two in windows 9x to nearly a dozen in windows 2000/XP/2003 (Derik J, Farmer 2006).

2.5 Registry Organization and Terminology

Burlington and Vermont indicated on his article that all values have names because there cannot be a null name. A value's name is analogous to a file's name. A value name can be up to 512 ANSI characters in length (256 Unicode characters), except for the special characters question mark (?), backslash (\), and asterisk (*). Furthermore, Windows XP/2003 reserves all value names that begin with a period (.). Just as no folder can contain two files with exactly the same name.

A full Registry might easily contain 15,000 keys and 35,000 values (Gralla, P.2007).

The Registry Editor interprets the number so the user sees the data type in plain Text. Table 1 shows each of the data types, their corresponding number, and a brief description of what the data type means.

Table 2.5: Registry Value Data Type

Data type	Number	Description
REG_NONE	0	Data type is not defined.
REG_SZ	1	Fixed-length text string expressed in user-friendly format, which is often used to

		describe components.
REG_EXPAND_SZ	2	Variable- or expandable-length data string.
REG_BINARY	3	Binary data that is displayed in the editor as hex.
REG_DWORD	4	32-bit double word values with bytes in reverse order. Since Intel already stores data in this format, this Term is synonymous with REG_DWORD and they have the same numeric value.
REG_DWORD_LITTLE_ENDIAN	4	32-bit double word value with bytes in normal order with the highest bit appearing first.
REG_DWORD_BIG_ENDIAN	5	32-bit double word value with bytes in reverse order with the highest bit appearing first.
REG_LINK	6	An internal-use-only data type for a Unicode symbolic link.
REG_MULTI_SZ	7	Multiple-string field in which each string is separated by a null (00), and two nulls (00 00) mark the End of the list of string.
REG_RESOURCE_LIST	8	Listing of resource list for devices or device drivers (REG_FULL_RESOURCE_DESCRIPTOR).we Can view but not edit these lists.

2.6 Registry Concepts

2.6.1 Why Registry Must Be Written Directly?

As Derrick J. Farmer outlined one of the first questions is what is the registry? The windows registry is a central repository or, more specifically, a hierarchical database of configuration data for the operating system and most of its programs. While creating a convenient central location for this data, it also creates the potential for a single point of failure that can bring the system to a halt.

Furthermore discussed, we can make deletion and modification directly in the registry, but many of the typical windows protection features, such as **redo, undo, and Recycle Bin** do not exist for the registry. This is also why the registry should be directly accessed and modified only by people who know what they are doing.

Because of the "single point of failure" vulnerability, the operating system uses safeguards to enable recovery to safe configuration through the Use of "last known good configuration" and restore points in windows XP. Also, usually the user doesn't interface directly with the Registry rather uses Windows utilities and configuration menus, such as those found in Control Panel, to make system changes that are stored in the Registry.

2.6.2 Making a Restore Point on Windows (Backup Windows Registry)

According to Microsoft Corporation on the System Restore function has been enabled. To do so we need to go to “My Computer”, Right Click and choose properties then Go to the system Restore tab, and make sure that the box adjacent to turn off System Restore has not been checked. If it has remove the check mark to enable it.

To create a restore point, we need to go to start - all programs - accessories - system tools - system Restore. Choose create a restore point, click next, and provide a name for the restore point, such as "Before I Touched the registry". When finished, we must click on create, and a restore point will be created. If for any reason there is need to return to this restore point, should simply go to the UI (User interface) for system restore and choose “my computer” to an earlier time. Next is, locate the name for restore point, and then follow the prompts to restore system.

The setting for restore points are stored in the Registry, which should come as no surprise. They are stored at
`HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWSNT\CurrentVersion\SystemRestore.`

To make this a viable feature, we must create restore points often enough to make them useful, and thus we will find that windows XP will create them every 24 hours and ME will create them every 10 hours of computer use or 24 hours of calendar time. Turning off a system for an extended period can throw this cycle out of synch, but one will be created shortly after the next system startup. The interval for restore point creation is stored in the `RPGlobalInterval` value, and the default `DWORD` data will be

86,400(seconds, since 24 hrs = 86,400 seconds). This can be changed but rarely is as if creating a system snapshot every 24 hours isn't cool enough from a forensic perspective, the default retention period is 90 days. That setting is stored in the RPLifeInterval value and has a default DWORD value of 7,776,000 (seconds, since 90 days = 7,776,000 seconds). The system restore folder is limited to 12 percent of hard drive, and this may impose a smaller retention period than 90 days. Think about this for a minute. We get a system snapshot every 24 hours that is retained for 90 days. This is starting to sound like a forensic gold mine and it is. System restore points can be turned off this is rare to find. The setting for disabling restore points is a value named DisableSR and it defaults to 0, meaning that restore points are being created. If the setting is 1, they have less than 200MB; the system restore service will automatically stop (Microsoft Corporation Tech net).

We can find restore points in numbered folders at \System Volume Information\restore[1]\RP##(where ## are sequentially numbered as restore points are created). Here are a few interesting facts about this folder:

The user can't access folders and files below \System Volume Information using the Explorer interface. This is true even if the user has administrator rights and hidden/system files are set to be visible. This condition makes it difficult for the average user to access, manipulate, or delete these files!

2.6.2.1 Restore Point Hack

That the reason why even the administrator can't access the folder \System Volume Information lies in the security permissions for this folder. Its default

configuration provides only system has right to this folder and its children. While the administrator has no rights to access this folder; the administrator can add "administration" to the permissions list for this folder, giving full control to the administrator (or any other user for that matter). Thus, if we want, as administrator, we could gain access to this folder by modifying the ACL or file security permission for the folder holding the System Restore folder and files. (Derrick J, farmer 2006)

2.7 Forensic Analysis of the Windows Registry

According to stated information of Lance Mueller (2007) there are 5 root keys (i.e. starting point) in Windows registry. Table 2 shows the root keys and the abbreviation normally used.

Table 1.7: Root and Abbreviation

Name	Abbreviation
HKEY_CLASSES_ROOT	HKCR
HKEY_CURRENT_USER	HKCU
HKEY_LOCAL_MACHINE	HKLM
HKEY_USERS	HKU
HKEY_CURRENT_CONFIG	HKCC

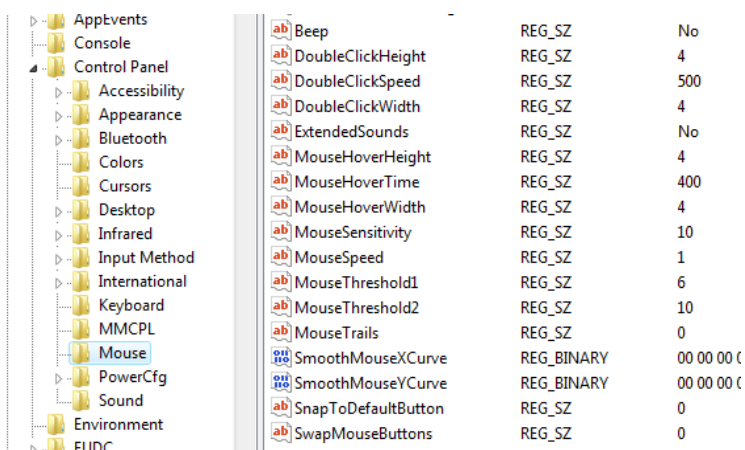
2.7.1 Value

Each key has one or more values. There are 3 parts in value, which are Name, Type and Data (Mueller, L 2007).

There are 6 primary types of the values that are displayed and modified in the Registry Editor (Gralla, P.2007):

String values (REG_SZ):

String values contain strings of characters, more commonly Known as text. They are the easiest to edit and are usually in plain English. In addition to standard strings, there are two far less common string variants, used for special purposes:



AppEvents	Beep	REG_SZ	No
Console	DoubleClickHeight	REG_SZ	4
Control Panel	DoubleClickSpeed	REG_SZ	500
Accessibility	DoubleClickWidth	REG_SZ	4
Appearance	ExtendedSounds	REG_SZ	No
Bluetooth	MouseHoverHeight	REG_SZ	4
Colors	MouseHoverTime	REG_SZ	400
Cursors	MouseHoverWidth	REG_SZ	4
Desktop	MouseSensitivity	REG_SZ	10
Infrared	MouseSpeed	REG_SZ	1
Input Method	MouseThreshold1	REG_SZ	6
International	MouseThreshold2	REG_SZ	10
Keyboard	MouseTrails	REG_SZ	0
MMCPL	SmoothMouseXCurve	REG_BINARY	00 00 00 00
Mouse	SmoothMouseYCurve	REG_BINARY	00 00 00 00
PowerCfg	SnapToDefaultButton	REG_SZ	0
Sound	SwapMouseButtons	REG_SZ	0
Environment			
FLINT			

Figure 2.7.1.1: Registry String Value

Multistring values (REG_MULTI_SZ):

Contain several strings (usually representing a list of some sort), concatenated (glued) together and separated by null characters (ASCII code 00). Individual characters in REG_ MULTI_SZ keys are also separated by null characters, so we'll actually see three null characters in a row between multiple strings.

Expandable string values (REG_EXPAND_SZ):

Contain special variables into which Windows substitutes information before delivering to the owning application. For example, an expanded string value intended to point to a sound file may contain %SystemRoot%\media\startup.wav. When Windows reads this value from the Registry, it substitutes the full Windows path for the variable, %SystemRoot%; the resulting data then becomes (depending on where Windows is installed) c:\windows\media\startup.wav. This way, the value data is correct regardless of the location of the Windows folder.

Binary values (REG_BINARY):

Similarly to string values, binary values hold strings of characters. The difference is the way the data is entered. Instead of a standard text box, binary data is entered with hexadecimal codes in an interface commonly known as a *hex editor*. Each individual character is specified by a two-digit number in base 16 (e.g., 6E is 110 in base 10), which allows characters not found on the keyboard to be entered. Note that hex values stored in binary Registry values are displayed in a somewhat unconventional format, in which the lowest-order digits appear first, followed by the next-higher pair of digits, and so on. In other words, the digits in a binary value are paired and their order reversed: the hex value 1B3 thus needs to be entered as B3 01. If we want to convert a binary value shown in the Registry Editor to decimal, we'll have to reverse this notation. For example, to find the decimal equivalent of 47 00 65 6e, set the Windows Calculator to hexadecimal mode and enter 6e650047, and then switch to decimal mode to display the decimal equivalent, 1,852,112,967.

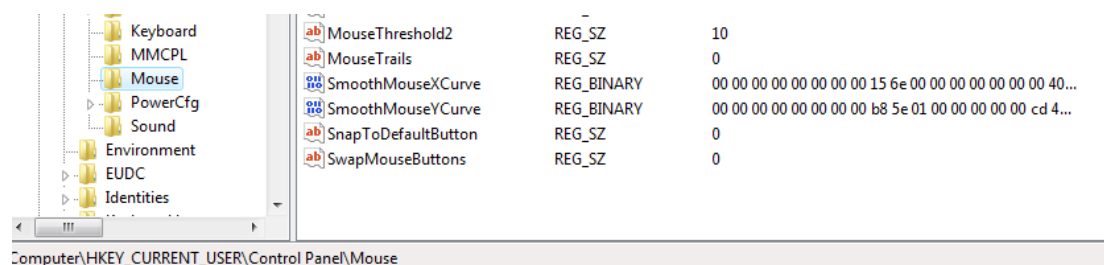


Figure 2.7.1.2: Binary Values

DWORD values (REG_DWORD):

Essentially, a DWORD is a number. Often, the contents of a DWORD value are easily understood, such as 0 for no and 1 for yes, or 60 for the number of seconds in some timeout setting. A DWORD value is used only where numerical digits are allowed; string and binary types allow anything. The DWORD format, like the binary type, is a hexadecimal number, but this time in a more conventional representation. The leading 0x is a standard programmer's notation for a hex value, and the number is properly read from left to right. The equivalent decimal value is shown in parentheses following the hex value.



Figure 2.7.1.3: DWORD Values

QWORD values (REG_QWORD):

This is much like a DWORD value, with one difference: it is a 64-bit value, rather than a 32-bit value like DWORD (Gralla, P.2007).

When an application read value's data in REG_BINARY from the registry, the application decides on how to decode the value. Application can store data in binary (using REG_BINARY type) using their own data structure, hence only the application knows how to interpret it. For instance, interpreting REG_BINARY data as 8-bitASCII or 16-bit Unicode could result in two different values. This technique could be used to hide data or at least confuse forensic examiner. Alternatively, some applications store REG_SZ and REG_DWORD data in REG_BINARY value, decoding and finding them can be difficult (Mueller, L 2007).

Offender can use this technique to hide data. Program can use four-byte REG_BINARY and REG_DWORD values (32-bit) interchangeably. Since Intel x86-based system uses little Endian architecture, REG_BINARY 0x01 0x02 0x03 0x04 is equivalent to REG_DWORD 0x04030201(Mueller, L 2007).

Regardless of value's type, the registry actually stores all values in binary format in the actual file. Since all values are stored alongside with their corresponding type, it allows the Registry Editor to interpret the value's data correctly.

2.8 Registry Root Key Organization

Anson Mueller (2007) depicts the two keys HKLM and HKU are the only root keys that Windows physically stores on files. HKCU is a symbolic link to sub key in HKU. HKCR and HKCC are symbolic links to sub keys in HKLM. Below are the brief descriptions of each 5 root keys.

2.8.1 HKEY_USER

HKU contains per-user (user-specific) information and setting. HKU contains at least these 3 subkeys:

- DEFAULT
- SID, SID is the security identifier for console user (user currently using the keyboard).
- SID_CLASSES contains per-user class registration and file association.

HKU has other well-known SID in Windows XP.

- S-1-5-18 refers to Local System account.
- S-1-5-19 refers to Local Service account. It is used to run local services that do not require Local System account.
- S-1-5-20 refers to Network Service account. It is used to run network services that do not require Local System account.

Any other sub keys in HKU are associated to secondary users. Windows XP has a feature called Secondary Logon, which allows user to run a program as a different user, usually with elevated privileged. Thus, user can logon to a limited account for daily routines and uses elevated privileged for occasional administrative task. The secondary user SID (usually administrative account SID) will only present in the HKU sub keys if the user performs a secondary logon during the user's session. If an offender performs a secondary logon on any other accounts, the secondary user sub key will exist in HKU until secondary user logoff, or the program running in the elevated privileged is closed (Anson Mueller 2007).

2.8.2 HKEY_CURRENT_USER

This entire branch is a mirror (or symbolic link) of one of the sub keys of HKEY_USERS (discussed shortly). This allows Windows and all applications to access and store information for the current user without having to determine which user is currently logged in. An application that keeps information on a per-user basis should store its data in HKEY_CURRENT_USER\Software and put information that applies to all users of the application in HKEY_LOCAL_MACHINE\SOFTWARE. Like many aspects of Windows, the Registry provides a mechanism for applications to store configuration data, but it does little to enforce any policies about how and where that data will actually be stored (Gralla, P 2007).

HKCU contains the computer users' settings. HKCU is actually a symbolic link to HKU/SID, the current console user's SID. This branch contains information on

environmental variables, desktop settings, mapped network drive settings, and application settings. Table 4 briefly describes some HKCU sub keys that are of potential forensic values (Anson Mueller 2007).

Table 2.8.2: HKCU Sub Keys

Subkeys	Descriptions
Environment	Each subkey corresponds to an environmental variable user has set.
Identities	Each Identities subkey corresponds to an identity in Microsoft Outlook Express. Outlook Express allows multiples identities (users) to use a single mail client. However, since Windows XP supports multiple user profiles, users rarely have to share their mail client.
Network	Each Network subkey corresponds to a mapped drive Windows connects during user system logon. Subkey name is the drive letter to which the network drive is mapped. The subkey contains configuration to connect the network drive.
Software	Contains user-specific application settings. Programs store their settings in a standard way, HKCU\Software\Vendor\Program\Version\. Vendor is program's publisher; Program is the Program's name; and Version is program's version.
Volatile Environment	Contains environmental variables that are defined when user logon to Windows XP.

2.8.3 HKEY_LOCAL_MACHINE

Steve Bunting further agrees the HKLM contains per-computer (computer-specific) settings which apply to all users logging into that particular computer.

Table 2.8.3: HKEY_LOCAL_MACHINE

Subkeys	Descriptions
HARDWARE	Stores information regarding hardware Windows XP detects during startup . The subkeys are dynamically created during system startup. They include information on device driver and associated resources.
SAM	Security Accounts Manager (SAM) is a local security database which contains local users and groups information. ACL prevents Administrator from viewing this subkey.
SECURITY	Contains Windows local security database in the SAM subkey. ACL prevents Administrator from viewing this subkey.
SOFTWARE	Stores per-computer application settings . Programs store their settings in this standard form, HKLM\Software\Vendor\Program\Version.

SYSTEM	<p>Contains control set, which contains device driver and service configurations.</p> <p>HKLM\SYSTEM\CurrentControlSet is a symbolic link to ControlSetXXX, and the key HKLM\SYSTEM\Select indicates which ControlSetXXX is in use.</p>
--------	---

2.8.4 HKEY_CLASSES_ROOT

On Forensic mastering book, Steve Anson and Steve Bunting discussed the HKCR contains two types of per-user settings, file associations, and class registration for Component Object Model (COM) object. File associations describes the file types and associated programs that open and edit them. HKCR consumes most of the space in registry. Windows merges two keys HKLM\SOFTWARE\Classes (contains default file associations and class registration) and HKCU\Software\Classes (contains per-user file associations and class registration) to obtain HKCR. In fact, HKCU\Software\Classes is a link to HKU\SID_Classes. By merging the two keys, program can register per computer and per-user file associations and program classes.

Contains file types, filename extensions, URL protocol prefixes and registered classes. We can think of the information in this branch as the “glue” that binds Windows with the applications and documents that run on it. It is critical to drag-and-drop operations, context menus, double-clicking, and many other familiar user interface semantics. The

actions defined here tell Windows how to react to every file type available on the system (Gralla, P 2007).

2.8.5 HKEY_CURRENT_CONFIG

HKCC is a symbolic link to current hardware profile configurations subkey, HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current. Current is a link to the key HKLM\SYSTEM\CurrentcontrolSet\Hardware Profiles\XXXX.

2.8.6 Registry Hives

From Shlomo Hersheop and Rew Honig stated information, Registry Editor only shows the logical structure of the registry. Physically, registry is not stored in a single file in the hard drive. Windows stores registry in a few separated binary files called hives. For each hives file, Windows creates additional supporting files that contain backup copy of the respective hives to restore the hives during failed system boot. Only HKLM and HKU has corresponding hives (since the rest are symbolic links). However, none of 5 root keys are directly associated to a hive file.

Table below shows registry path and their corresponding hives on disk. All hives in HKLM are stored in %SYSTEMROOT%\System32\config\ (%SYSTEMROOT% usually refers to C:\WINDOWS).

HKLM\HARDWARE is a dynamic hive that is created each time the system boots and it is created and managed entirely in memory. HKU\DEFAULT hive file correspond to %SYSTEMROOT%\System32\config\default. HKU\SID hive file is stored in user home directory, which is %USERPROFILE%\NTUSER.DAT, while HKU\SID_CLASSES hive file correspond to %USERPROFILE%\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat. Table 6 describes the actual hive files and the supporting files extension.

Table 2.8.6.1: Registry Path – Hive and Supporting Files

Registry Path	Hive and Supporting Files
HKLM\SAM	SAM, SAM.LOG
HKLM\SECURITY	SECURITY, SECURITY.LOG
HKLM\SOFTWARE	software, software.LOG, software.sav
HKLM\SYSTEM	system, system.LOG, system.sav
HKLM\HARDWARE	(Dynamic/Volatile Hive)
HKU\DEFAULT	default, default.LOG, default.sav
HKU\SID	NTUSER.DAT
HKU\SID_CLASSES	UsrClass.dat, UsrClass.dat.LOG

Table 2.8.6.2: File Extension and Description

File Extension	Description
No extension	Actual Hive File
.alt extension	Backup copy of hive, used in Windows 2000, not XP
.log extension	Transaction log of changes to a hive
.sav extension	Backup copy of hive created at the end of text-mode (console) phrase during Windows XP setup

2.8.7 Registry Search

The windows registry editor has a search feature the Edit menu. With this feature, we can search for data in the registry. We can limit the search to keys, values, or data, or we can search all the areas. Each value contains data of a specified data type specified by a number (Burlington, Vermont, A).

The Registry has thousands of keys and values, which makes finding a single key or value rather laborious. Luckily, there are a few alternatives that will greatly simplify this task. First, we can simply search the Registry. Start by highlighting the key at the top of the tree through which we want to search, which instructs the Registry Editor to begin searching at the beginning of that key. (To search the entire Registry, highlight

“Computer.”) Then, use Edit → Find, type in what we’re searching for, make sure that all the “Look at” options are checked, and click Find Next.

Another shortcut is to use the keyboard. Like Explorer, when we press a letter or number key, the Registry Editor will jump to the first entry that starts with that character.

Furthermore, if we press several keys in succession, all of them will be used to spell the target item. For example, to navigate to: HKEY_CLASSES_ROOT\CLSID\

{20D04FE0-3AEA-1069-A2D8-08002B30309D}

Start by expanding the HKEY_CLASSES_ROOT key. Then, press C + L + S quickly in succession, and the Registry Editor will jump to the CLSID key. Next, expand that key by pressing the right-facing arrow, or by pressing the right arrow key, and press { + 2 + 0 (the first three characters of the key name, including the curly brace), and we’ll be in the neighbourhood of the target key in seconds (Gralla, P 2007).

2.9 Registry Improvement

2.9.1 Registry Improvement on Windows Vista

Microsoft Corporation tech net further agrees that several new registry files have been added to Windows Vista. The following list represents all the registry hives on a default Vista system:

C:\Boot\BCD

C:\Windows\System32\config\RegBack\SECURITY

C:\Windows\System32\config\RegBack\SOFTWARE
C:\Windows\System32\config\RegBack\DEFAULT
C:\Windows\System32\config\RegBack\SAM
C:\Windows\System32\config\RegBack\COMPONENTS
C:\Windows\System32\config\RegBack\SYSTEM
C:\Windows\System32\config\BCD-Template
C:\Windows\System32\config\COMPONENTS
C:\Windows\System32\config\DEFAULT
C:\Windows\System32\config\SAM
C:\Windows\System32\config\SECURITY
C:\Windows\System32\config\SOFTWARE
C:\Windows\System32\config\SYSTEM
C:\Windows\winsxs\x86_microsoft-windows-b...-bcdtemplate-
client_31bf3856ad364e35_6.0.6000.16386_none_25edb26a062d63a9\BCD-
Template

The user's NTUSER.DAT file is still located in the root of the user's root folder (C:\Users\<username>). Notice that Windows Vista now uses the "REGBACK" folder instead of the "REPAIR" folder that Windows 2000/XP/2003 use for backup copies of the registry.

2.9.1.1 Registry Virtualization on Windows Vista

Mueller Lance (2007) illustrates that Windows Vista now contains a feature called “registry virtualization” as part of a security enhancement. This feature ensures that users who are not administrators cannot write the certain parts of the registry, especially during software installation. If a program tries to write to a specific registry key that is protected, the installation program will be seamlessly redirected to a “virtual” registry key contained within the user’s personal registry hive (NTUSER.DAT). Any write attempt by a non administrator to the: HKEY_LOCAL_MACHINE\Software registry key(s) causes the system to redirect the write into a virtual store in the user’s profile:

HKEY_USERS\<User SID>\Classes\VirtualStore\Machine\Software

In a simple definition Windows Vista handles that in several ways: (Gralla, P.2007)

When a standard user tries to run the Registry Editor, User Account Control (UAC) springs into action, asking for an administrator password. If one is provided, the Registry Editor can be used and changes made. If none is provided, the Registry Editor will not be allowed to run, and no changes will be made.

When a standard user installs software, UAC will ask for an administrator password. If the user provides one, the software will make the appropriate changes to the %SystemRoot% and %ProgramFiles% folders and to the Registry.

If a legacy application fails to work correctly with UAC, Vista will use a new feature called *file and Registry virtualization*. This will create virtual %SystemRoot% and %ProgramFiles% folders, and a virtual HKEY_LOCAL_MACHINE Registry entry. These virtual folders and entry are stored with the user’s files.

So the Registry itself—as well as the *%SystemRoot%* and *%ProgramFiles%* folders—are not altered in any way, so system files and the Registry are protected.

2.10 Registry Investigation with Forensic Tool

On this stage we are discussing on one of the tools available for forensic investigators with its features specially have been made for forensic job and the reasons we choose this tool plus the other tools to extract the information from registry keys.

2.10.1 Encase Registry Forensic

Mathew Geiger as well as Steve Anson proposed Encase Registry Analyzer which is a computer forensics tool used by many computer forensic examiners and intrusion investigators. Depending on the Environment, we may be doing both the computer forensic and the network investigation. In other environments, the functions are segregated. Regardless, if we have EnCase available, it is an excellent tool to use to examine the Windows Registry. Registry hive files are compound files that are mountable in Encase. As with any other mountable file within the Encase environment, we need only right-click one of the hives files and choose them to view its file structure. Before we mount the file, however, we must first locate it. Encase makes this task very easy using the conditions feature. Go to the filters pane, navigate to the conditions Tab, and double-click the registry file condition, which is located in the system files folder.

With this condition set, activate the set included folders trigger at the device level, and the registry files will appear in the table view pane.

To mount any of the hive files, simply right-click the desired file and choose to view its file structure, since some of these files are Very large and complex, mounting them may take some time, but usually less than a minute. When the file mounts, we can navigate through the various keys as would any hierarchical files condition to locate the hive files, before we can navigate and see values in the table Pane, we'll need to turn off that condition by clicking on it on the toolbar. When a value is displayed in the table view pane, we will see its name in the name column, its data type in the file type column, and its data in the view pane in either the next or hex view.

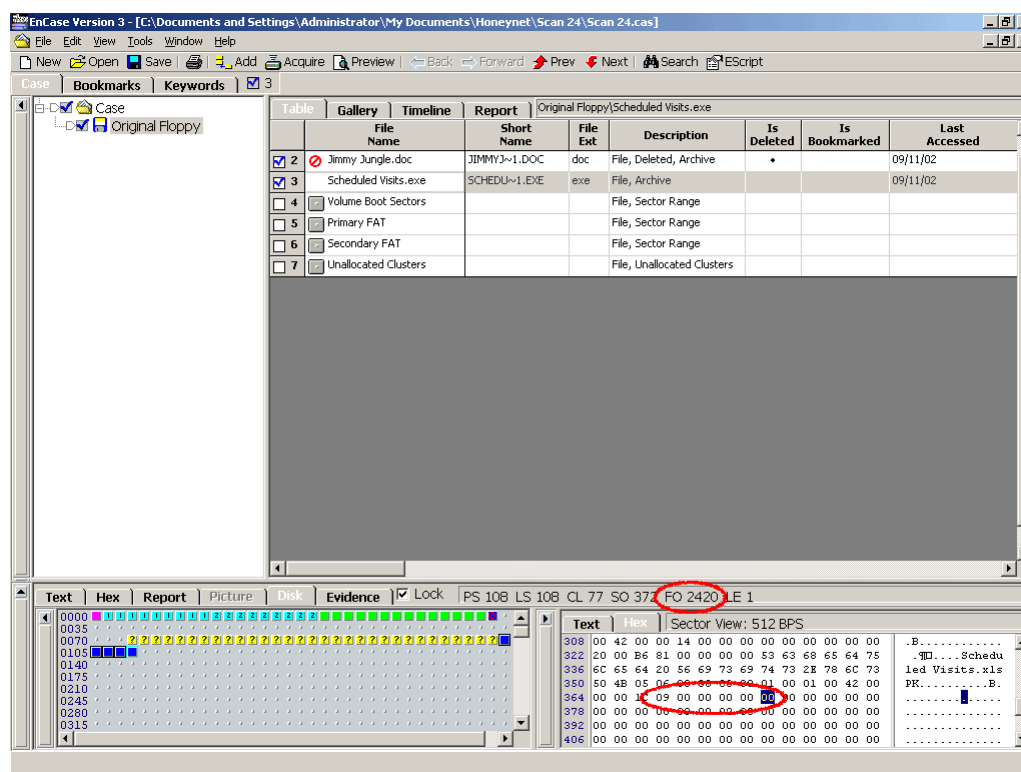


Figure 2.10.1: Encase Forensic Tool

In addition to manual examination of the windows registry, EnCase offers several EnScripts that mount the registry, extract information, and then unmount the registry when finished. The results of these EnScripts are most often found in the bookmarks view. EnScripts are an excellent way to pull out routine information as well as other specialized information from the registry, saving considerable time and energy.

The windows initialize Case EnScript extracts a large volume of information from the registry that is useful in almost any situation. It's important for the investigator to determine time zone information. NTFS as well as most of the timestamps found in the registry are stored natively in Greenwich Mean Time (GMT). The operating system displays local times to the user as an offset to GMT based on the user's local Time zone offset stored in the registry. For example, let's say an event occurs on February 1, 2007, 1800 hrs in GMT. To display the time to the user, The operating system subtracts the EST offset (GMT -0500) from 1800 hours and display it as 1300 hours. If we are examining media that was set to as different time zone than the current one, we must account for this to be accurate. If a machine was set on PST (GMT -0800) and examined in EST (GMT -0500), the times will be off by three hours unless the local machine is set for PST. EnCase allows us to make this adjustment internally at the Volume, disk, or case level so that we can examine and adjust disparate time zone within a uniform context.

2.10.2 Why Choosing Encase

Encase Enterprise provides all the functionality for effective response identified by NIST (National Institute of Standards and Technology) (Guidance Software 2004).

Immediate response capability: a key benefit of Encase is its revolutionary ability to conduct immediate and through forensic of any system on a wide area network, without disrupting operations which enables organizations to better contain and mitigate incidents as they occur.

Initial system snapshot: is a central feature of Encase enterprise specifically designed for rapid and through incident response analysis.

Analyze live system with minimal invasiveness: is the Encase ability to analyze live system in a forensically sound manner without taking those systems off-line, or being visible to the user or the attacker.

Volatile data acquisition and analysis: Encase supports this critical aspect of incident response by quickly obtaining and displaying all the relevant volatile data like open ports, open files, running processes and the live registry. Encase capture and examine the volatile data from several systems at once.

Forensic hard drive data acquisition: Encase is adept at obtaining complete and accurate forensic images of hard drives (tested by NIST). Encase can create these images on a local drive or any computer on a wide area network.

Computer forensic analysis: Encase provides industry leading computer forensic analysis capability.

Establish a proper Chain of custody with a message Digest Hash Algorithm:

The Encase acquisition process features an integrated process to establish a proper chain of custody, including the secure generation of a MD5 hash for the forensic image and CRC's for every 32k of data for authentication.

Log file acquisition and analysis: Encase supports the collection, parsing and analysis of log files maintained by various systems and appliances throughout the organizations network. Furthermore the deleted file and log files recovery functionality is one of the Encase abilities.

Ability to correlate multiple time zones of acquired media: Encase is specifically designed to support the analysis and correlation of dates and times originating in different time zones with integrated correlation tools and a timeline viewer.

Validated computer forensics technology via courts and independent testing: Encase is specifically accepted by the courts in appellate and trial court decisions. And NIST is one of the many agencies that have independently tested and validated the Encase program.

2.10.3 Using CAIN to Decrypt the Protected Storage System

Mark Russionovich suggested the Cain software which can decrypt the auto filled data on forms browser or whatever field that have ever been set for being auto completed. So for downloading this software should go to: <http://www.oxid.it/cain.html>.

This tool is distributed as compiled binaries, so there is no telling what all it may do to the system without extensive tool analysis. And before downloading or installing it is probably better to turn off the antivirus on system. And we'll have the option to load the winpcap drivers to enable our NIC to function in promiscuous mode.

So we should navigate the storage data from menu and to extract the data from the local host's protected storage, click the toolbar button marked with a + sign. If the auto complete option is enabled we can see the stored data. If not the auto complete option is disabled. The registry key on:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU.

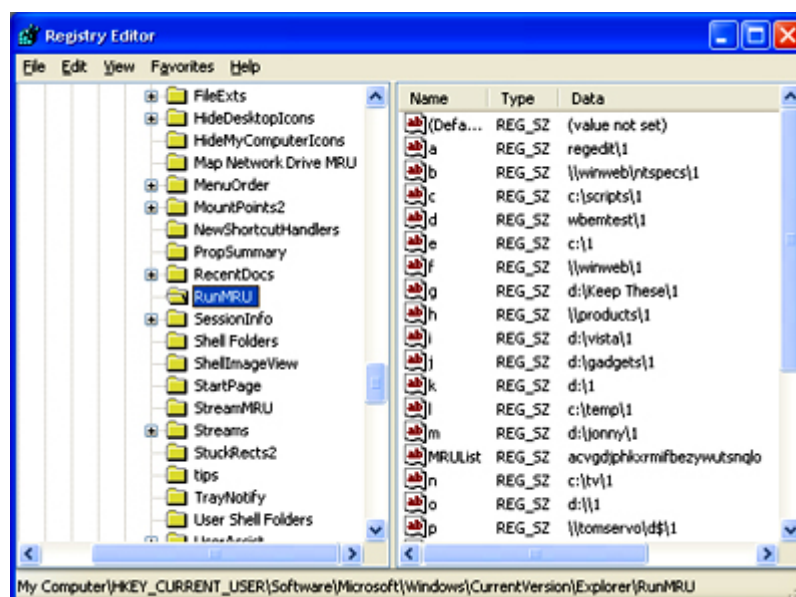


Figure 2.10.3: Protected Storage System (MRU)

In the value pane, we can see the various commands listed as values a, b, c, and so on. The MRU List value describes the order as string of those lettered value names,

with most recent being listed first and the oldest last. We'll find the advanced users make use of the Run command often, and that includes intruders when using their computer or a victim's computer. If we are looking at this key with a tool that parses and displays the last-written time for this key, we'll also know when the most recent command in this list was run.

If we look carefully we will notice that the Map Network Drive MRU key appears a few entries before the RunMRU key. This key contains a listing of the most recently mapped networked drives. This can be important in a network-intrusion investigation as we'll want to know what other machines were connected to the compromise, because a trusted connection already exists. This key works much the same way as the previous MRU key. The various mapped drives are listed as values named a, b, c, d, and so on. Once again if we are viewing this data with a tool that displays the last-written timestamp for this key, we'll know when the most recent drive in the list was mapped.

Other MRUs:

HKCU\Printers\Settings\Wizard\ConnrctMRU: list most recently used network printers by user.

HKCU\Software\Microsoft\Windows\Currentversion\Explorer\ComDlg32: last visited MRU lists program and the files opened by them. OpenSaveMRU lists files opened and saved, grouped by extension; there is a key named for each in the list.

HKCU\Software\Microsoft\Windows\searchAssistant\ACMr: contains two subkeys that store searches carried out in Windows Explorer, which is useful in

determining if the user/intruder was searching his local or networked drives for files/ directories or words/ phrases, with the former stored in key 5603 and the latter in key 5604.

2.10.3.1 Disabled Most Recently Used (MRU) Files List by Hackers

In the meantime by Microsoft Corporation Tech Net, there are certain circumstances in which hackers disable the list of most recently used files for privacy or security reasons. To disable this list, they follow these steps:

1. Using the registry editor, navigate to the
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Policies\Comdlg32 key.
2. Create a REG_DWORD value named NoFileMru and set this value to 1.

2.11 Manually Information Extraction

Many of the registry keys have forensic evidentiary value which can be derived through simple searched and export them. On this part we are reviewing the literatures have relative information about this subject to make the output of this study more complete.

2.11.1 Finding Information on Software Key

Steve Anson and Steve Bunting (2007) outlined that the information found in the software key (HKLM\SOFTWARE) is located in the hive file named SOFTWARE, as shown in figure 2.11.1. This file is found in the path %SYSTEMROOT%\system32\config and should not be confused with the software key found in the HKEY_CURRENT_USER key, abbreviated HKCU. The HKLM\SOFTWARE key contains software setting for the local machine; while HKCU\SOFTWARE contains software setting that are users specific. Although both are important, our current focus is on the local machine software setting.

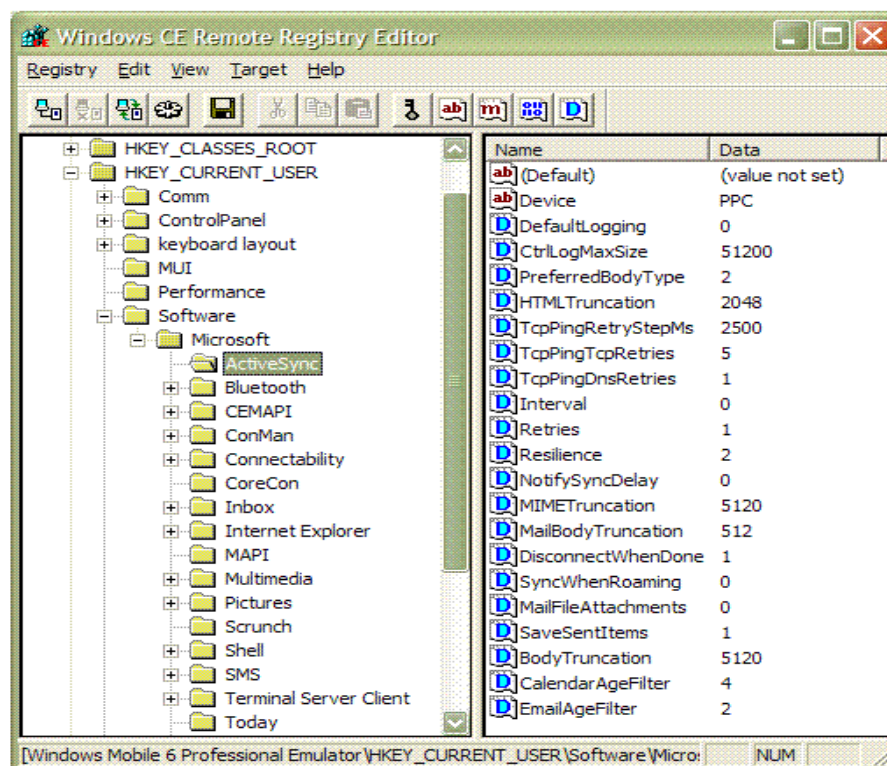


Figure 2.11.1: Software Key

2.11.2 Installed Software

When program are installed on a computer, a registry entry is usually associated with that software installation. Oddly enough even when software is removed or uninstalled, the registry entries persist, making the registry, once again, and a rich source for evidentiary data. Software installation entries are varied in both name and location. If we don't know exactly what we are looking for, it is best to look in many different locations known to contain information about software on a system.

The first location to look at is the root of the software key itself. Program located here may be obvious by their name, or they may be more obscure, being listed under an innocuous or even bogus company name. Often these bogus names are obvious when we see them, but we have to look to find them.

Other locations to examine for software are the following two registry keys:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App
Paths and
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\currentVersion\Uninstall. The former lists the paths to the various installed application.

Software are often installs an "uninstall" key that provides information for program removal. The latter key,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\currentVersion\Uninstall, usually contains this information. It is not uncommon to find a program listed in one of these registry areas but not in the other. The network-sniffing and password-cracking

tool Cain is not seen under the keys, yet its uninstalled information is clearly listed under C of the uninstall key.

2.11.3 Last Logon

When it's important to determine who last logged on to a system, we can find this information in the HKLM\SOFTWARE key but more specifically at HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. The value name DefaultUserName stores the username of the last-logged-on user so that it can be displayed as the default username for the next logon (Mathew Geiger 2006).

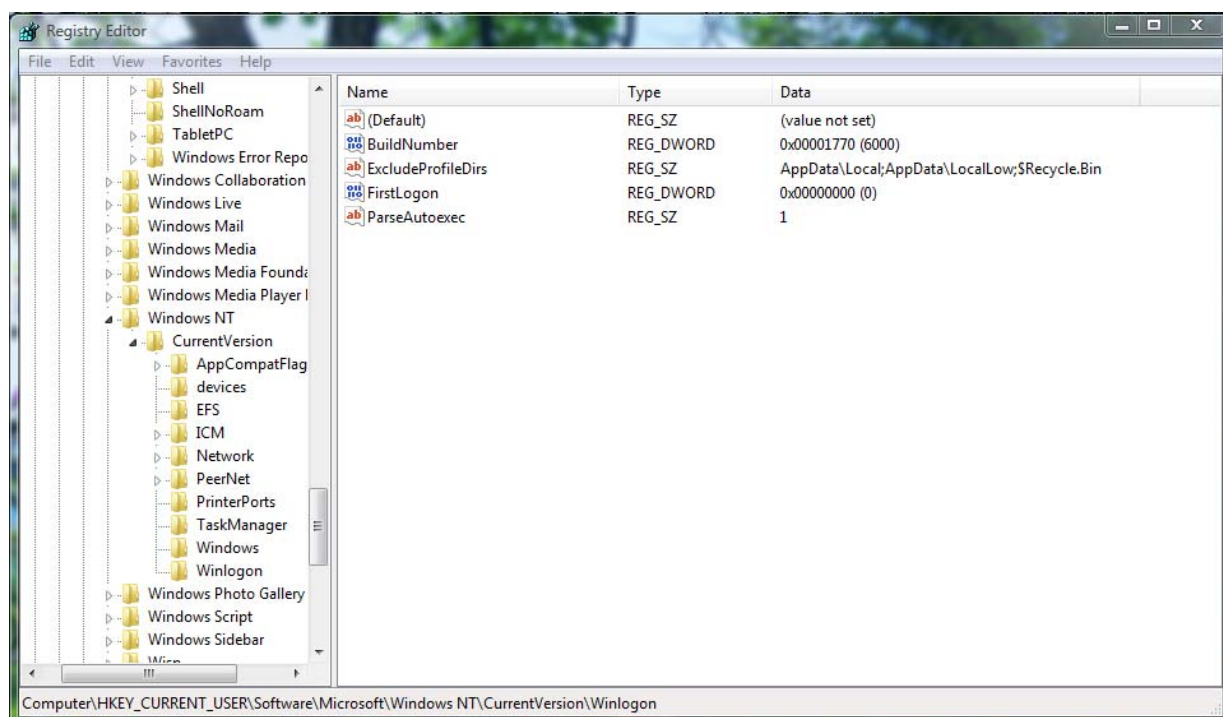


Figure 2.11.3: Winlogon

2.11.4 Windows Firewall Logging

The windows firewall has an excellent logging feature; however, in keeping Microsoft tradition, by default it is turned off. When enabled, it can log dropped connections, successful connections or both. The log is stored in plain text and is located at the path %systemRoot%\pfirewall.log. The log size is also configurable. Don't overlook this potential evidence, because the user or administrator may have had it enabled. (Youngoo kim, Sangsu Lee, Dowon Hong, 2006)

2.11.5 Exploring Security Identifiers

Meanwhile by Steve Anson and Steve Bunting (2007), each user, group, and machine in a Windows environment is assigned a security identifier (SID). The SID is a unique identifier in that no two SIDs are the same. Windows grants or denies access and privileges to system objects based on access control lists (ACLs), which in turn use the SID as a means of identifying users, groups, and machines, since each has its own unique SID.

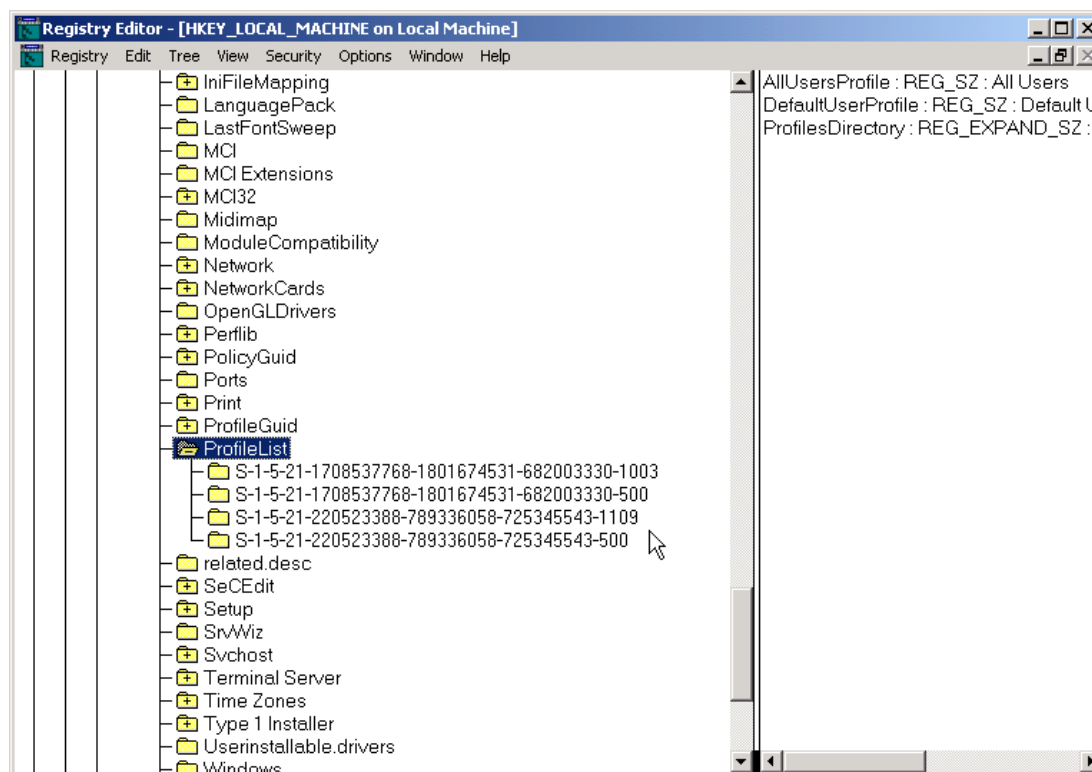


Figure 2.11.5.1: SID Number

The SID number we are seeing in this example is S-1-5-21-1708537768-1801674531-682003330-1003. As we have in the following, each part of this number has a meaning or purpose. The first part is the first and only letter in the string, which is S and is shown here in bold. The S simply means that the string that follows is an SID. The second part is the revision number, which is currently always 1(bolded here in: S-**1**-5-21-1708537768-1801674531-682003330-1003). The third segment is the authority level from 0 to 5. In the present example, it is a 5 (bolded herein: S-1-**5**-21-1708537768-1801674531-682003330-1003).the fourth part is the longest segment in the example and is the domain or local computer identifier (bolded herein: S-1-5-**21-1708537768-1801674531-682003330**-1003). This string uniquely identifies the domain or local computer. This string can be, however, as short as one field for the well-known SIDs. The fifth and the final part is the relative identifier (RID), which will be a unique

number within the domain or local computer. In the example is 1003(bolded herein: S-1-5-21-1708537768-1801674531-682003330-**1003**)

We can resolve this SID to its user in several ways. If the user is locally authenticated (non-domain logon), the SID-to-user resolution is carried out in the local SAM (security account manager). The SAM file is a security database of hashed passwords and usernames that is also a registry hive file. If the user is logged on to a domain, the SID-to-user resolution occurs in the active directory of the domain controller.

The registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList provides a listing of subkeys, each named after SIDs on the system. If a user has interactively logged on to the machine, using a local or domain account, there will be a subkey with that user's SID for its name. This subkey is created at the time of the first interactive logon (making it a great place to identify accounts that have interactively logged onto a computer). When we locate the SID in question, there will be a value for that subkey named profileImagePath. The string data for this value will list the path to the user's profile, part of which will be the previously named registry key.

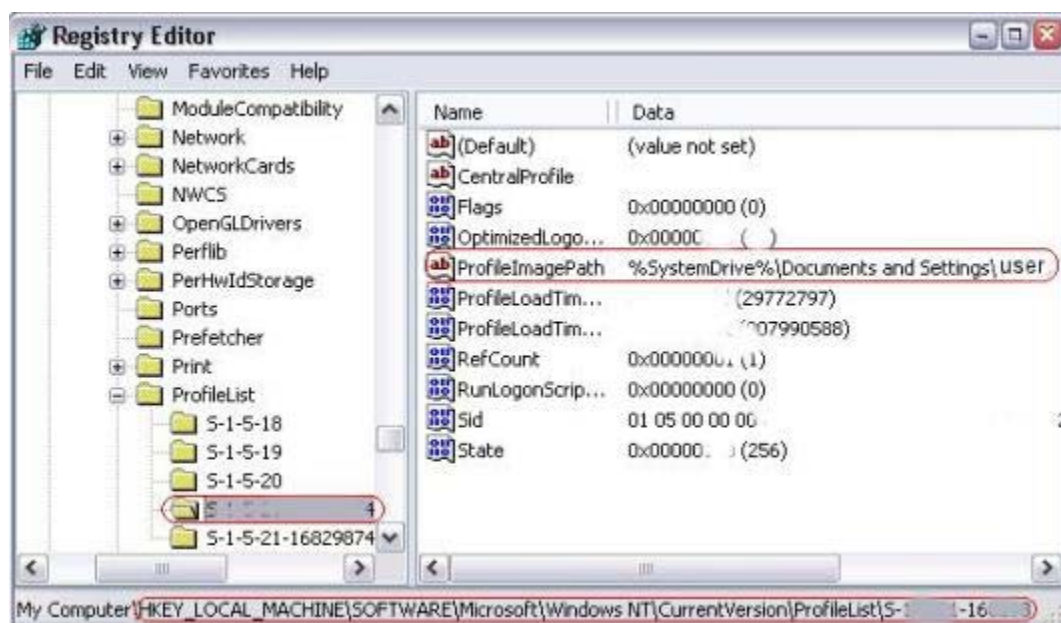


Figure 2.11.5.2: SID Numbers and Profile Image Path

2.11.6 Investigating User Activity

Hor Cheong Wai (2006) discussed more that the user's NTUSER.DAT file is loaded with data indicative of the user's preferences and activity. Just as the SOFTWARE hive file listed software installed on the computer, the software key of the NTUSER.DAT file contains keys for software installed on the computer. Just as those keys in the local machine SOFTWARE hive file contain entries for software long since deleted, the user's software key likewise contains entries of installed software. In addition, the user's software key contains data specific to the user. This data can be in the form of searches, usernames, passwords, commands, programs run, or string entered, and the list goes on. We'll cover some of the more common and significant data that is specific to the user. As we go through this list, keep in mind that we always can go to the

restore points and capture this data at specific points in time, which can be a tremendously valuable source of often overlooked evidence.

Because investigators and examiners always want to locate passwords for a host of reasons, let's look first at the protected storage System provider area of the registry. This Registry key stores the AutoComplete data for Microsoft Internet Explorer. The data is encrypted; however, the encryption is far from being complex. The auto complete feature can store three different types of information, depending on the selections made by the user. The purpose of this feature is to assist the user by remembering from data that is frequently encountered, and it prevents a lot of repetitive typing. Also, this feature assists the user by remembering usernames and passwords. As with any benefit, there is often a cost, which in this case is privacy and security. To access to this option we should go to this address: Tools-Internet Option-Content-AutoComplete.

2.11.7 Registry Last Write Time

By the information stated by Lih Wern Wong (2006), all registry key has a value called Last Write time, which is similar to file's last modification time. In fact, this value is a FILETIME structure, which is the same as file's MAC (Modified, Accessed, and created) time.

The FILETIME structure is a 64-bit value representing the number of 100-nanosecond intervals since January 1, 1601 UTC (MSDN, 2005c). However,

investigator could only obtain the registry key LastWrite time, but not the registry value LastWrite time(mention it in discussion) . The LastWrite time will be updated whenever a registry value in the key is created, modified or deleted. Tool such as Keytime.exe (Carvey, 2005a) allows examiner to retrieve LastWrite time of a specific key. Knowing the time of a key is modified or created allows forensic investigator to infer the approximate time an event or activity occurred. For instance, if a suspicious registry value is found in the registry's Run key, investigator could query the LastWrite time of the key and compare it to the MAC time of the file to which the registry value is pointing. If there is a match between the key LastWrite time and the MAC time of the file to which the registry value is pointing, investigator will know the time the registry value was created. The figure2.11.7 Indicates a sample of exported registry last write time exported from registry.

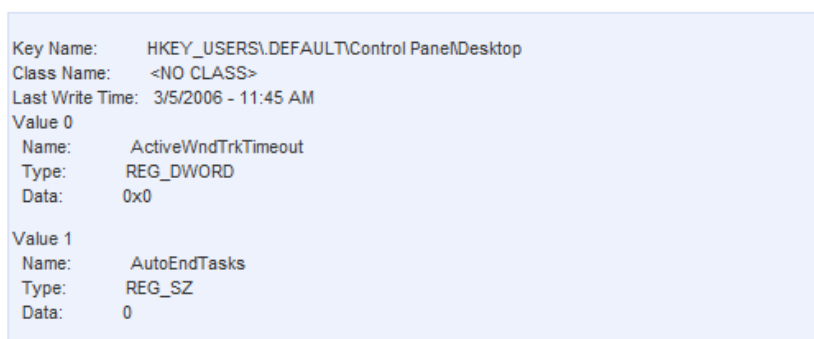


Figure 2.11.7: Registry Last Write Time

2.11.8 The Key Value Corresponds Remote Desktop Running

The question often arises, with increasing frequency as remote desktop hacks become more prevalent, as to which registry key determines whether remote desktop was enabled.

HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\TERMINAL SERVER. There is a value in this key named fDenyTSConnections. If we enable remote desktop, its value will be 0, meaning the terminal services connections are not being denied, meaning they are being permitted. (Mark. R and Bryce. C, 2006).

2.11.9 The keys are used For Automatic Program Startup

Programs that are not services, or in other words, programs that are started within the user logon session, may be started under any of the following keys: (Microsoft Corporation tech net, 2006).

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
 HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
 HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
 HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
 HKCU\Software\Microsoft\Windows\CurrentVersion\Run
 HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
 HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices
 HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnc

2.12 Recover from a Corrupted Registry

In most cases it will be necessary to overwrite the corrupted Registry with a good backup copy of the Registry. In certain cases it may be possible to boot the system using the last known good configuration in a few cases it may be possible to use the Regcln utility to fix minor inconsistencies (Microsoft Corporation tech net, 2006).

2.13 Registry Protection

The only real way to protect the Registry is to back it up to disk or tape daily. We should also perform a Registry backup prior to:

Installing or upgrading any applications or operating system components. Adding any new devices, using the Registry Editor, There is a second type of protection that of securing the Registry against spoofing, modification, and ensure by unauthorized users. In its default configuration, Windows NT is easy to use but very insecure. If we are in a network environment, we probably need better security than what NT's out-of-the-box configuration offers (Microsoft Corporation tech net, 2006).

2.14 Ease of Use or Security

On The comparison has been done by Michael Cobb (2007), there is some differences on registry configuration between different operating systems such as Mac OS X , Linux, Sun Microsystems' Solaris operating system. We prepared all issues in a table to make the comparison and their reason more clear. The main reason of bringing this table is to know how different the windows registry with other operating system is.

Table 2.14: Ease of Use of the Security

Operating systems	Approach	Disadvantages	Advantages
Windows	Binary Format Store Machine and users file in separate files	<ul style="list-style-type: none"> - Standardizing - Protecting the database - ACL permissions should be configured to lock down remote registry access and limit user access to keys. - Inevitable registry grows cause slow down the startup and finally unstable 	<ul style="list-style-type: none"> - Configuration backup and restore actions involve only a small number of files in known locations. - administrators can use Group Policy to centrally manage program and policy settings - self maintaining and self-repairing,

		- Corruption will affect wide reaching effects.	
Mac OS X	Standard flat files using the XML format.	- Ease of use and availability and the cost	- Corruption will affect single application - NetInfo is the system database stores system wide setting and network configuration.
Linux	Flat text files XML format, /etc and /var directory	Not easy to use for every one	Secure
Sun Microsystems' Solaris	XML namespace can be accessed by network repository service such as NIST,LDAP,NFS or Local directory	Not easy to use for every one	Secure

2.15 Forensic value Of Registry Keys

The following section highlights some of the important registry keys in Windows XP (Service Pack 2) and how they can be of benefit to help describing suspect activities on the computer by Mathew Geiger (2006).

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

MRU is the abbreviation for most-recently-used. This key maintains a list of recently opened or saved files via typical Windows Explorer-style common dialog boxes (i.e. Open dialog box and Save dialog box) (Microsoft, 2002). For instance, files (e.g. .txt, .pdf, htm, .jpg) that are recently opened or saved files from within a web browser (including IE and Firefox) are maintained. However, documents that are opened or saved via Microsoft Office programs are not maintained. Subkey * contains the full file path to the 10 most recently opened/saved files. Other subkeys in OpenSaveMRU contain far more entries related to previously opened or saved files (including the 10 most recent ones), which are grouped accordingly to file extension (Mathew Geiger).

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU

This key correlates to the previous OpenSaveMRU key to provide extra information. Whenever a new entry is added to the previous OpenSaveMRU key, registry value is created or updated in this key. Each binary registry value under this key contains a recently used program executable filename, and the folder path of a file to which the program has been used to open or save it. If a file is saved, the folder path refers to the saved file destination path; if a file is opened, the folder path refers to the file source path. New registry value will only be created to this key, if no existing

registry values contain the program executable filename. However, if there is a matching executable filename in the existing values, only the folder path section of the related registry value is updated (Mathew Geiger).

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

This key also maintains list of files recently executed or opened through Windows Explorer. This key corresponds to %USERPROFILE%\Recent (My Recent Documents). The key contains local or network files that are recently opened and only the filename in binary form is stored. It has similar grouping as the previous OpenSaveMRU key, opened files are organized according to file extension under respective subkeys. In addition, the Subkey Folder contains the folder (without drive letter and parent folder) of the recently open files. Subkey NetHood which corresponds to %USERPROFILE%\NetHood contains only LAN shared folder path (server and folder name) which the file was opened. However, deleting this RecentDocs key does not removed the content in both folders %USERPROFILE%\Recent and %USERPROFILE%\NetHood (Mathew Geiger).

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

This key maintains a list of entries (e.g. full file path or commands like cmd, regedit, compmgmt.msc) executed using the Start>Run commands, as shown in Figure below. The MRUList value maintains a list of alphabets which refer to the respective values. The alphabets are arranged according to the order the entries is being added "services.msc" which correlates to "g" is the most recently added entry, while "taskmgr" is the earliest. However, most recently added entry does not imply most recently used command as suspect may have reexecuted previous commands. Windows does not modify the key LastWrite time or MRUList if there is an existing entry in the key. If a file is executed via Run command, it will leaves traces in the previous two keys OpenSaveMRU and RecentDocs. Deleting the subkeys in RunMRU does not remove the

history list in Run command box immediately. However, when either button Start>Log Off or Turn off Computer is clicked (without actually logging off or shutdown), the respective entries in Run history list are then removed. By using Windows “Recent Opened Documents” Clear List feature via Control Panel>Taskbar and Start Menu, suspect can remove the Run command history list. In fact, executing the Clear List function will remove the following registry keys and their subkeys:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\HKCU\Software\Microsoft\Internet Explorer\TypedURLs\

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU

Name	Type	Data
(Default)	REG_SZ	(value not set)
a	REG_SZ	notepad\1
b	REG_SZ	notepad.exe\1
c	REG_SZ	cmd\1
d	REG_SZ	taskmgr\1
e	REG_SZ	regedit\1
f	REG_SZ	telnet\1
g	REG_SZ	services.msc\1
MRUList	REG_SZ	gebcefd

Figure 2.15: MRU on Registry

HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management

This key maintains Windows virtual memory (paging file) configuration. The paging file (usually C:\pagefile.sys) may contain evidential information that could be removed once the suspect computer is shutdown. This key contains a registry value called ClearPagefileAtShutdown which specify whether Windows should clear off the paging file when the computer shutdowns. By default, windows will not clear the paging file. However, suspect may modify this registry value to 1 to signify paging file clearing during system shutdown. Forensic investigator should check this value before shutting down a suspect computer during evidence collection process (Mathew Geiger).

HKCU \Software\Microsoft\Search Assistant\ACMru

This key contains recent search terms using Windows default search. Subkey 5603 contain search terms for finding folders and filenames, while subkey 5604 contain search terms for finding words or phrases in a file.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

Each subkey in this key represents an installed program in the computer. All programs listed in Control Panel>Add/Remove Programs correspond to one of the listed subkeys. However, they are other installed programs (e.g. device driver, Windows patch) that are not listed in Add/Remove Programs. Each subkey usually contains these two common registry values – DisplayName (program name) and Uninstall String (application Uninstall component's file path, which indirectly refers to application installation path). Other possible useful registry values may exist, which include information on install date, install source and application version (Mathew Geiger).

HKLM \SYSTEM\MountedDevices

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CP C\Volume

The first key contains a list of mounted devices, with associated persistent volume name and unique internal identifier for respective devices. This key lists any volume that is mounted and assigned a drive letter, including USB storage devices and external DVD/CDROM drives. From the listed registry values, value's name that starts with "\DosDevices\" and ends with the associated drive letter, contains information regarding that particular mounted device. For instance, if the binary data for registry value "\DosDevices\F" contains "\"??\Storage#RemoveableMedia" at the beginning of the value, it signifies a USB removable disk was connected to the system USB port. By correlating the entry with registry key LastWrite time, investigator would know when the removable device is connected. The second key also contains similar information as MountedDevices key, which is located under the respective device GUID (Globally Unique Identifiers) subkey and in the binary registry value named Data (Mathew Geiger).

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR

This key contains addition information about list of mounted USB storage devices, including external memory cards. This key when used in conjunction with two previous keys will provide evidential information. To illustrate the method, assume a USB thumb drive named "USB Card IntelligentStick" with serial number "20000101061325-00" was connected to a suspect system. USB storage device unique serial number can be acquired via UVCView program, under the field "iSerialNumber". However, not every USB thumb drive has a serial number. This key will have a subkey containing device name, such as "Disk&Ven _USB _Card&Prod _IntelligentStick&Rev _1.00 ". Under this subkey is the device ID subkey which contains the device serial number; "20000101061325-00&0". The latter subkey has a ParentIdPrefix value (data="7&1064d032&0") which corresponds to the binary registry value in HKLM \System\MountedDevices; \DosDevices\F for instance. The latter value will contain

binary data similar to "\\?\Storage#RemoveableMedia#7&1064d032&0". By mapping this two key, forensic examiner will know which USB device (using device serial number) is mounted to which drive letter. Apple iPod devices leave similar trace (Mathew Geiger).

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce

This first key usually contains programs or components paths that are automatically run during system startup without requiring user interaction. Malware usually leaves trace in this key to be persistent whenever system reboots. Subsequent four subkeys may also contain suspicious entries. Similar 5 sets of "Run" registry keys may exist under root key HKCU, pertaining to the logged on user configuration.

HKLM\SOFTWARE\Microsoft\Command Processor

HKCU\Software\Microsoft\Command Processor

This key has a registry value named Autorun, which could contain command that is automatically executed each time cmd.exe is run. However, modification to this key requires administrative privilege. Malware exploits this feature to load itself without user's knowledge. Suspect could also covertly run a malicious program under the cover of cmd.exe, by setting the Autorun data to the executable file path.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

This key has a registry value named Shell with default data Explorer.exe. Malware such as Krbot appends the malware executable file to the default value's data, modifying it into Shell=Explorer.exe %system%\System32.exe to stay persistence across system reboots and logins. Suspect could append executable file path to this registry value to run program covertly as done by Trojan Watson. Furthermore, there is another registry value in this key named TaskMan which allows user to run an alternate task manager. Though by default it is not created in Windows XP, suspect can create it and point it to an executable file. Both registry values are executed automatically whenever the system boots. Suspect can utilize these two registry values to run program secretly. However, modification to this key requires administrative privilege.

HKLM\SYSTEM\CurrentControlSet\Services

This key contains list of Windows services. Each subkey represents a service and contains service's information such as startup configuration and executable image path. Some malware such as BackOrifice2K will install itself as service. Thus, it leaves trace in this key.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

This key allows administrator to map an executable filename to a different debugger source, allowing user to debug a program using a different program. Modification to this key requires administrative privilege. Suspect could exploit this feature to launch a completely different program under the cover of the initial program. First, suspect creates a subkey named for example, notepad.exe (taskmgr.exe, compmgmt.msc or any benign looking executable). Then under the subkey notepad.exe, suspect creates a new string (REG_SZ) value named Debugger, and directs it to an undercover program (e.g. C:\Windows\system32\telnet.exe). When the suspect executes notepad.exe, telnet client is launched instead of Notepad. If the suspect runs notepad.exe

through Windows Run for instance, its history list will only shows notepad.exe. Thus, suspect could use this technique to deceive forensic examiner. Suspect could also redirect the initial program to a Trojan version of the program which launches a backdoor whenever the initial program is run. Malware exploits this feature to load itself without user's knowledge (Mathew Geiger).

HKCR\exefile\shell\open\command

This key contains instruction to execute any .exe extension file. Normally, this key contains one default value with data “%1“%* (ShaolinTiger, 2003). However, if the value's data is changed to something similar to somefilename.exe "%1" %*, investigator should suspect some other hidden program is invoked automatically when the actual .exe file is executed. Malware normally modify this value to load itself covertly (File Extensions, n.d.). This technique apply to other similar keys, including

HKEY_CLASSES_ROOT\batfile\shell\open\command

HKEY_CLASSES_ROOT\comfile\shell\open\command

HKCR\Drive\shell

HKCR\Folder\shell

These two key contains subkeys that refer to menu items in Windows context menu. The first key points to the context menu when right clicking on Windows drive letter, while the second key refers to folder's context menu. Suspect could create a key to launch command prompt from the drive letter context menu, through key HKCR\Drive\shell\cmd\command\ . It is a very helpful feature especially if users need to open command prompt at folder level, via HKCR\Folder\shell\cmd\command. By default, Windows does not have this key. The default registry value has data cmd.exe /k "cd %L". Suspect could append for instance && notepad.exe to this value to launch both programs at once. However, the second program (notepad.exe) is loaded within the same

cmd.exe window (cmd.exe is not fully loaded until notepad.exe is closed). By modifying the default registry Value's data to cmd.exe /k "cd %L" && start notepad.exe , the two programs are launched separated under different windows. Thus, the second program can be loaded covertly (Mathew Geiger).

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID

This key contains network adapter recent settings such as system IP address and default gateway for the respective network adapters. Each GUID subkey refers to a network adapter. The data is retained even though the network connection is disconnected.

HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\GUID

This key contains wireless network information for adapter using Windows Wireless Zero Configuration Service. Under the GUID subkey, there are binary registry values named Static#0000, Static#0001, etc. (depending on the number of listed SSID) which correspond to the respective list of SSID in “Preferred Networks” box in Wireless Network Connection configuration. The registry value contains the SSID name in binary form. If registry value Active Settings contains an SSID name, it may signify last connected SSID. However, the result is not consistent when tested. If suspect connect to wireless networks using other 3rd party program that is usually bundled with the network adapter, instead of using Wireless Zero Configuration, no trace is left on this key. Forensic examiner can use this key with the previous network adapter GUID key to determine the last assigned IP address (Mathew Geiger).

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MapNetwork Drive MRU

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

The first key maintains a list of mapped network drive, including the server name and shared folder (Shannon, 2004). The value in this key is still retained even though the mapped network drive has been permanently removed or disconnected. In addition, permanent subkey (unless manually removed from registry) regarding mapped network drive is also created in the second key, and the subkey is named in the form of ##servername#sharedfolder.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

This key contains two GUID subkeys. Each subkey maintains a list of system objects such as program, shortcut, and control panel applets that a user has accessed. The GUID subkey beginning with "5E6" corresponds to IE toolbar, while subkey starting with "750" pertains to Active Desktop. However, registry values under these subkeys are weakly encrypted using "ROT-13" algorithm which basically substitutes a character with another character 13 position away from it in the ASCII table. Even though each registry value is not associated with specific time and date the event occurred, it could imply suspect has accessed certain file or object. For instance, the existence of an attack tool's filename on the entries could indicate suspect is trying to execute the malicious tool (Shannon, 2004).

HKCU\Software\Microsoft\Protected Storage System Provider

Windows Protected Storage is maintained under this key. Protected Storage is a service used by Microsoft products to provide a secure area to store private information. Information that could be stored in Protected Storage includes MSN Explorer and Internet Explorer AutoComplete strings and passwords, Microsoft Outlook and Outlook Express accounts' passwords, and MSN Messenger password. Registry Editor hides these registry keys from users viewing, including administrator. There are tools that allow examiner to view the decrypted Protected Storage on a live system, such as Protected Storage Pass View (NirSoft, 2004) and PStoreView (PStoreView, 2005).

AccessData Registry Viewer is capable of accessing and decrypting the subkeys in an offline manner (Lih Wern Wong, 2006).

2.16 LSA Secrets

The stated information on Mastering Forensic by Steve Anson and Steve Bunting indicates more that LSA stands for Local Security Authority. The security hive key is part of the Registry, although we can't access this key through Regedit. The key (SECURITY\POLICY\Secrets) contains security information regarding various accounts and other accounts necessary for the operation of Windows and is stored in this location by the service control manager. Windows must start many services when it boots, and every service or process on the system must run within some security context. Since service run without overtly activated by a logged in user, the system stores the credentials for service accounts so that they can automatically be launched under the appropriate account. It is, therefore, the job of LSA Secrets to store these security credentials. LSA Secrets are encrypted and stored on disk in the Registry, but Windows decrypts them upon boot and stores them in clear text in the memory space allocated to the LSA process. If we can locate and access that memory space, we can read the clear-text security credentials that are stored in RAM.

Many tools can extract this information from LSA and be run within the context of administrator. So theoretically there is no harm for administrator because he is the owner of the system and has the right to access the system's information. However, many exploits convey system or administrator security rights by vitiate of the exploit.

Therefore, an intruder with administrator rights can attack this security information from the LSA memory space.

Why would an intruder need this information if she already owns the system? The goal of most hackers is to continually expand their compromises to other machines. Most machines are connected to other machines in the network world. Those connections are for services, and those services and connections required cached or stored security credentials, many of which are stored in the LSA secrets. Thus, if the intruder can obtain security credentials for various machine or service accounts, she can expand her compromise to other hosts. Also Windows NT and 2000 by default cache the logon credentials for the last ten logons and this information will store in LSA Secrets.

There are many tools can extract LSA secrets, as instance **lsadump2** is a command line tool that will do the job. **Cain** is another one. So far we know that LSA secrets will be a target for an intruder who can expand her level of compromise on network; she will need to have administrator rights to extract this information. If she use tools such as lsadump2 or Cain, we'll likely see trace evidence of their use in the registry. If we do detect the use of such tools, we would now know of their significance, and we'd certainly have to expand the investigation to other connected hosts. May be we can find evidence on LSA secrets, for example usually some of them activate a guest account, giving it administrator privileges on the system. If there are cached login information credentials in the LSA secrets for such accounts, this can be valuable information.

2.17 Finding Clear-Text Password in the Swap File

Steve Anson and Steve Bunting discussed some useful information that Clear-text passwords are often found in the swap file and the hiberfil.sys file. The swap file is used to store RAM contents when RAM space is full. Thus RAM data, complete with clear-text passwords, is often written to swap file, resulting in clear-text passwords being written to disk. When the computer is placed on hibernate modes, the entire contents of RAM are written to the Hiberfi.sys file.

2.18 Discovering IP addresses

IP addresses are stored in the registry, which should come as no surprise by now. In fact, we can find not just current IP address but also recently used IP configuration. They are stored in the key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces`. Under this key, we will find many that are given GUID names. Under these GUID-named keys we will find various interface configurations for IP addresses that have been configured on the machine. They will exist for either static (fixed or assigned by the network administrator) or dynamic (assigned on the fly by a DHCP). IP addresses, we can determine which type by examining the setting for the interface (Steve Anson and Steve Bunting, 2007).

Figure 2.18 shows a static IP address. In the left pane, we can see the GUID-named key. In the right pane, among other values, we can see that enabled DHCP is set to zero, meaning that dynamically assigned IP address are not being assigned. The IP

address value shows the fixed IP address. The default Gateway value describes the Gateway router for this configuration. Other value provides other information that may be important to the investigation. And since registry viewer resolves the last written timestamp for this key, this information can likewise be important to the investigation (Derrick J Farmer and Burlington Wermont, 2006).

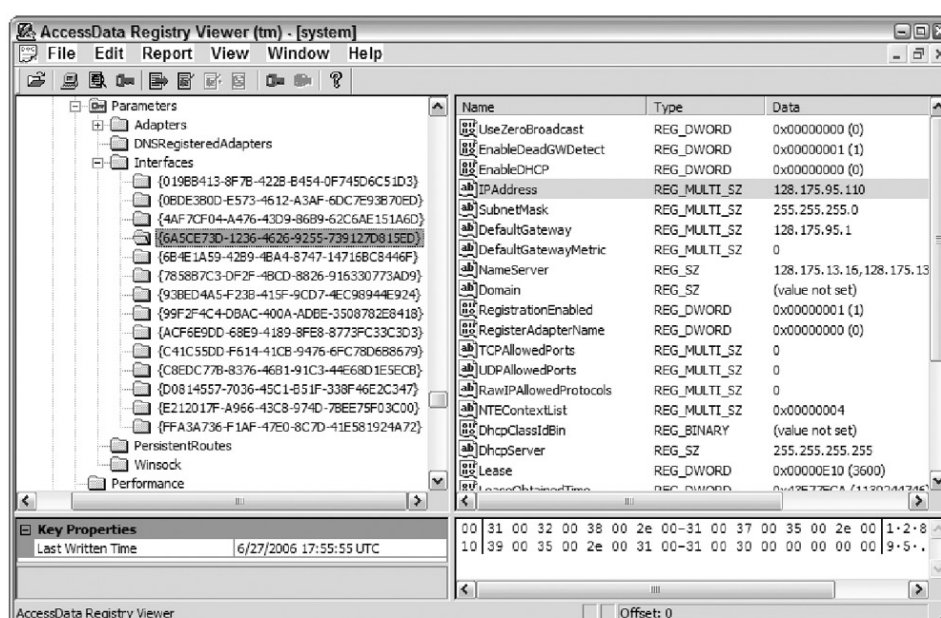


Figure 2.18: IP Addresses And Configuration

Chapter 3

Research Methodology

3.1 Introduction

Project methodology is fundamental in accomplish this project as it provides a certain method and guideline to ensure that the project is conducted in a well managed and firm manner. The research methodology discussed in this chapter define what are the activities that will be conducted throughout this project and what are the processes involved to successfully complete this project.

Based on the specification and requirements of each type of research, the methodology which is needed to be followed differs. Specific known research methodologies may be customized and adapted by researcher in order to appropriately address the requirement of a certain research.

Based on James E. Mauch in his book [22], the research methodology which is relevant to our problem is Analytical as well as Quantitative method. Analytical Because of using available facts and information and analyse them to make critical evaluation and Quantitative because it's base on measurement of quality or investigating certain phenomena among the quantity of registry keys. Since the aim of this project is to prepare registry forensic investigation guideline through analyzing various aspects of registry, the main plan of this guideline development is indicated thorough these Methodology approaches. So the main steps in the methodology shown in figure 3.1, below:

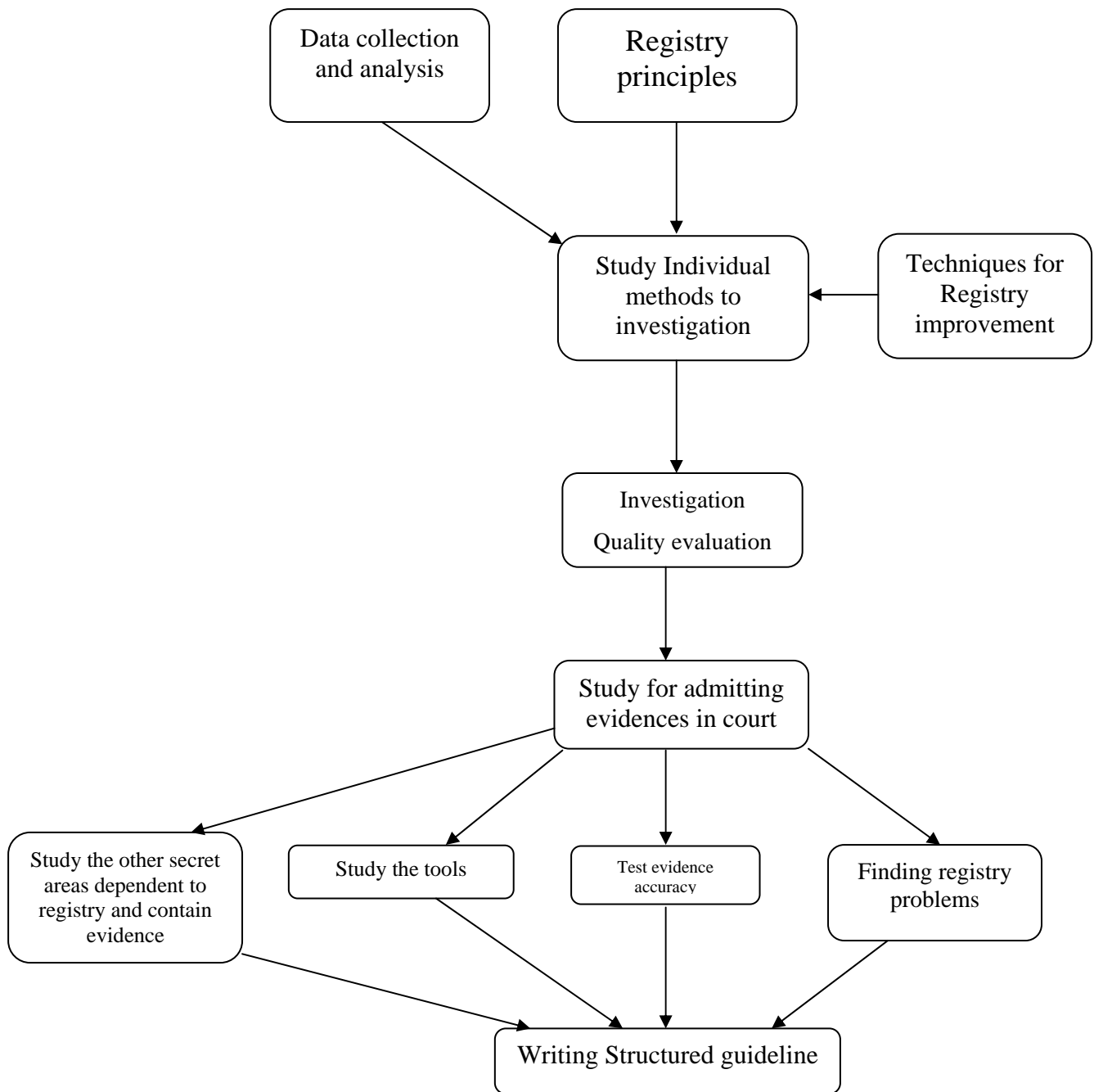


Figure 3.1: Research Methodology Adopted

3.2 An Analysis of Registry Principles

At first we define the principals of the registry and the ways to find the information through this channel. Knowing the structure of this section is required to successfully perform investigation job on windows registry. So by the definition of registry keys, hives, value the steps will apply more clear. By referring to literature review all the required principals has described to get the forensic analysis on next chapters. Some of the steps on this stage can be taken are:

- Finding the proper topic suitable with project implementation. So based on the scope, objective and problem we decided to choose the scope as “DEVELOPMENT OF DIGITAL FORENSIC GUIDELINE FOR WINDOWS XP AND VISTA REGISTRY”.
- The project objectives and project scope are identified and evaluated according to supervisor’s consent. The objectives are in the way to reach the aim like analysis of registry keys, data collection. Also the scope needs to be cleared, some areas like files which are inside the windows are not included in scope and we are concentrating on registry keys and its files.
- Assessing the key milestones in registry platform due to finding proper evidences and project requirement toward completing the guideline structure. For example the keys with higher value in being evidence are more important to be considering in guideline and there are some requirements like studying the evidence management basic information to make the guideline structure.

- Identifying and assessing the problems and their background to conduct the ideas and solutions. Problem identification is crucial to set the project objective and project scope during the work to find evidences.

3.3 Study the Individual Methods to Investigation

Reviewing the existing literature comes next after the specific topic has been chosen. A more clear understanding on research topic will be obtained as existing literature are analyzed so that we can become more familiar with the topic. Internet is the main resources to gather literature reviews, online journals and research articles that are ready made available to get the individual methods regarding to this topic and the problems solving. Here online database resources such as IEEE Explore, ACM Portal, Microsoft Tech net articles, and Emerald Text Online are accessed and utilized. On the current project by having many resources on windows registry forensic the work flow is going to analyze articles related to this topic and promote the idea belong to improvement security based point of view.

Beside of this part of study the improvements have maiden on windows vista registry will be discussed to be involved on analyze to get the ideas and solutions.

3.4 Techniques for Registry Improvement

At this stage we will take a look to the techniques cause registry environment more secure and improved. For example in Windows Vista the registry platform is more improved than Windows XP and it has more authentication on registry access by administrator with certain techniques has added in Windows Vista. So the security of registry on Windows Vista is more reliable than Windows XP. We will consider all the possible improvements to make users more updated from recent technology improvement.

3.5 Investigation Quality Evaluation

After having enough idea about the keys on Registry we will know that some of the keys and some of the approaches are more valuable and popular to finding information about hackers, so then we know the ways cause us to conduct better investigation with better quality which we will study on this project. For example there may be 5 ways to find the IP address from attacker machine but also there is one way cause us to derive the IP address from attacker machine plus the MAC address which has more worth and has more quality to be admitted in court, and of course the investigators need to know the best ways to make the time and price shorter. So these steps will be taken by searching through registry keys.

3.6 Study Evidences for Admitting in Court

One of the important points are having evidences which are able to be admitted in court so the keys and their correspondence data or evidence must be in the way of achieving admitted evidence at courts. That's why we need to seek for the data which are founded in this scope not out of it because many keys can have some information but may be they don't have ability to be admitted at courts. For example the data which will be cleared after refreshing the desktop or restarting the machine and it's at the time there is no feature to preserve them.

3.7 Study the other Secret Areas

Some of other places in windows XP and Vista are related to registry and have valuable information, like swap files and LSA secret so we will study them through available forensic articles and then try to take a look to these areas and have experiment to have better evaluation of investigation approaches.

3.8 Study the Tools

The tools available on the registry investigation have to be searched as well to understand their approach to find the evidences and their current process based on

registry forensic. The concepts why we are going to use the tools is the reason depends to the time, accuracy the management and ability to admit to courts. So after verifying the current famous tools we must provide the guideline from evaluated tool. The tools are like Encase, Regmon.exe, ART advanced Registry Tracer, Access Data's Registry Viewer.

3.9 Finding registry problems

On the way we have survey to achieve the aim the problems of registry which we face will be discussed on discussion chapter. These problems are related to the guideline make us having trouble to reach evidences. For example during the key searching to find evidences absolutely we face some problems like having time for every value on registry forensic evaluation which is one of the problems.

3.10 Test Evidence Accuracy

Of course we cannot take the evidences we are not sure about their accuracy on bringing data from hackers. So we need to add a stage which is testing all derived evidences then when their accuracy of having valuable data is acceptable we can consider them as part of guideline.

3.11 Writing Structured Guideline

Based on all information collected and tested regarding to their usage on forensic, guideline draft will be written on this stage. There would be need to some resources to write guideline in better manner and scale. After writing has been done, it is revised to make sure that the guideline itself is aligned with registry forensic investigation objectives and before starting to write such guideline we must make sure that the structure of this guideline is acceptable structure.

Chapter 4

Guideline

4.1 Introduction

A guideline is a document that aims to streamline particular processes according to a set routine. On this project the forensic registry guideline is an essential part of the larger process of computer digital forensic and since the aim of this project is making registry forensic investigation guideline, the output would be in sort of guiding for its defined users to have proper evidence processing. For example the users of this guideline which will be defined later will refer to this guideline to know how they can find certain information from certain keys without wasting their time by searching the registry platform and having complicated process to find them. For instance he wants to find the IP address of the machines been connected to his system, so he will search for the header of the section of guideline which corresponds by finding such information. And this information can be found under hardware section of the registry platform.

Since the computer evidences are fragile by their nature the purpose of preparing this guideline is make users to have a complete understanding of the technical Windows

Registry issues so then they can make the right decisions about Registry security risk management and Windows registry evidence processing issues in Windows XP and Vista registry scope.

Elements of the evidence life cycle include:

- Discovery & recognition
- Protection
- Recording
- Collection
- Identification (tagging/marking)
- Preservation
- Delivery
- Presentment of evidence in court
- Return of evidence to owner

For the purpose of court proceedings (whether criminal or civil), the best types of evidence are the Direct or Primary evidence. So the registry keys are from this kind if they being recognize and preserve well.

So we need to have a structure for this guideline and define how user is going to find related information from guideline.

On figure below we have defined the structure of this guideline, so the user which will be defined in coming pages will refer to the guideline by purpose of finding related information from headers. The header of each part indicates the information we can find from its specific key. Before user refer to the key a brief information about what he can find from this key is written below there, and at last the step which user needs to take to find and preserve the evidence.

The structure of this guideline is in below figure:

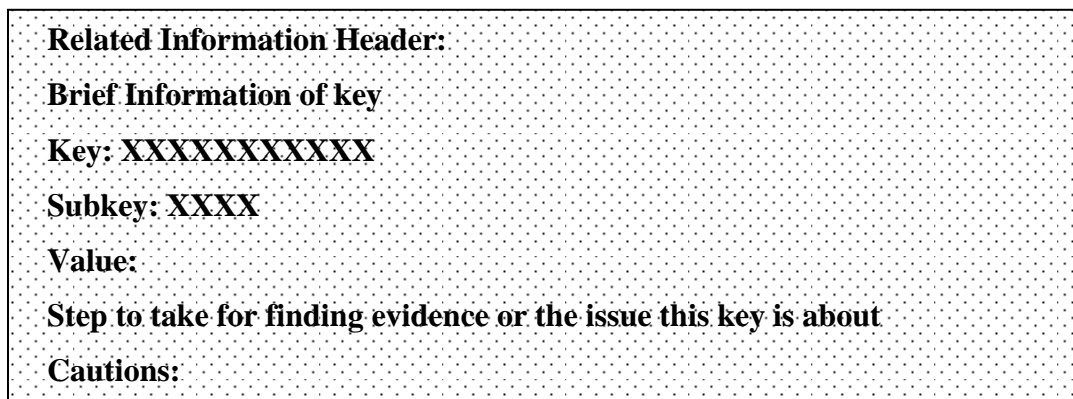


Figure 4.1: Guideline Structure

But before we go to the investigation part some of the mains steps like protection, recovery and Boted computers investigation, like other evidence management streamlines are included at the first part of guideline.

We need remember that these guidelines do not represent 'the only true way' to find and preserve the evidences. And also we should consider that many of the keys on registry platform can have the information but the collected keys and designed them as in this guideline the keys which are more related to the forensic value have been listed.

4.2 Audience and Assumptions

Two kinds of users are considered in this guideline:

- The users are assumed to have a basic grounding in classical computer forensics involving individual computer systems (e.g., personal computers) and network

servers with general information around Windows registry. So the Guideline is like manual searching through Registry keys.

How to read the guideline:

For defined users above the guide line is divided to four main sections and the streamline are conducted under related sections, which are: Hardware, Software, Windows and Security.

The places where the evidences embedded assumed as below:

- The information embedded in subkeys name, like a tool's name embedded in a subkey's name and can indicate a malicious tool.
 - The information embedded in predefined values and subkeys which indicate to evidence by considering its data.
 - The information embedded in Data part of a value which should be converted to the text using available tools to filter hex or binary values or using the simple export way.
-
- The Encase specialists who have the complete knowledge of Encase tool and need to have a guideline of Windows XP and Vista registry. In this case we assume the Encase users have enough experience on Encase and on the guideline they refer to the steps which are needed to be taken to find, preserve and report the evidence.

4.3 Experiment of Guideline Production

First of all we had study on registry platform and its environment to get familiar with the scope of registry to know how to search the keys, how is the categorization of the keys and how to extract information from keys. And for the investigation with tools we had study in different tools and their methodology in finding evidences and their ability.

The experiment of Registry keys analysis is base on the searches and the studies we have through different aspects and articles. The searching of the keys simply refers to search the keys, sub keys, their name, value and Data. The search between these points and choosing them to be inside the guideline is base on the forensic value the may have. Also we have categorized the guideline to four section hardware, software, windows and security base on the search we have among the keys.

So by refer to the guideline we will see that every key indicated an evidence having a format which first we found the key based on the search we had for each of them and then we tried to study the information it contains from itself and related documents, then based on the format we tried to sort them in the structure we have defined.

Another approach to search and find the forensic value of registry keys are the related articles, for example if there is an article arguing about the some problems forensic examiners have with certain key in registry environment we have considered the way we can find evidence from that key to extract the value of that key rather than speaking about another points.

Although Windows vista has improvement in forensic science and its abilities to help forensic examiners more than previous versions but we must consider the keys improvements and their change in windows vista. For example one of the keys has been added to windows vista is:

HKEY_USERS\<User SID>\Classes\VirtualStore\Machine\Software

That indicates the virtual state of the writing aim to the registry by non administrators, so we extracted the forensic aspects of this key and related information it can have inside the guideline. The keys mostly are based on the windows Xp and for the times there are differences between two version investigations we have included the way of investigation for Windows vista as well.

4.4 Implementation Digital Investigate Via Encase

On this stage the search approaches will be explained and surveyed and explore the keys and hives from Encase digital forensic tool. We will be more familiar with environment, functionalities, usability, how to investigate from registry keys, how to work on registry keys, and more of this software. This project study is specially on the registry section of windows so the parts of Encase we are working is just for registry whereas this tool can have a broad investigate on windows with various abilities.

4.5 GUIDELINE:

4.5.1 Windows XP and Vista Registry Platform Keys Guideline

Protection:

In many forensic discussion articles one of the main parts must be consider is first the protection of systems before any incident happen to investigate. Also the registry environment needs to be protected from many dangers are around of it.

Four particular steps must be taken to protect the registry environment are as below:

- 1- Cleaning the registry on a regular basis by using Registry Cleaner tools.
- 2- All registry cleaners work the same way. The more problems they find the better the cleaner.
- 3- Full registry backup and restore is enough to keep us out of trouble.
- 4- All the care the registry needs is cleaning and repairing.

Precaution: Make Registry Restore Point Before Manual Investigation

The registry key are very sensitive, removing one critical key or value can cause the system not boot or get serious damage so we recommend to make a restore point before touch the registry environment.

On My Computer, Right Click and choose properties then Go to the system Restore tab, and make sure that the box adjacent to turn off System Restore has not been checked. If it has remove the check mark to enable it.

To create a restore point, go to start - all programs - accessories - system tools - system Restore. Choose create a restore point, click next, and provide a name for the restore point, such as "Before I Touched the registry". When finished, click on create, and a restore point will be created. If for any reason we need to return to this restore point, simply go to the UI (User interface) for system restore and choose my computer to An Earlier Time. Next, locate the name of the restore point, and then follow the prompts to restore the system.

Registry Recovery after incident happened:

To recover the registry we need to go to “My Computer”, Right Click and choose properties then go to the system restore tab (system protection tab in windows vista), and make sure that the box adjacent to turn off System Restore has not been checked. If it has, remove the check mark to enable it.

To create a restore point, we need to go to start - all programs - accessories - system tools - system Restore. Choose create a restore point, click next, and provide a name for the restore point, such as "Before I Touched the registry". When finished, we must click on create, and a restore point will be created. If for any reason there is need to return to this restore point, should simply go to the UI (User interface) for system restore and choose “my computer” to an earlier time. Next is, locate the name for restore point, and then follow the prompts to restore system.

To make this a viable feature, we must create restore points often enough to make them useful, and thus we will find that windows XP will create them every 24 hours and ME will create them every 10 hours of computer use or 24 hours of calendar time. Turning off a system for an extended period can throw this cycle out of synch, but one will be created shortly after the next system startup.

The system restore folder is limited to 12 percent of hard drive, and this may impose a smaller retention period than 90 days.

Search Registry

To search inside windows registry we need to highlight the most probably key place which can have what we want to search in, and then push the find key and the searching word from right click.

To Extract Registry Key Last Write Time

To extract the last write time go to the key we want to know it's time and then export the key from view menu with .txt extension file type.

It is usually important to have date and time information about that software when possible. Often intruders will alter the modified, accessed, created (MAC) times on their software files, making them appear as though they have been on the system for months or years. The registry stores last-written timestamps for various keys. If we can determine when a particular malware software registry key was last-written, particularly an uninstall key, we can likely use that information to determine when the intruder was active on the target system. With that information, we can examine

various logs pertaining to network activity and begin the process of tracking the intruder back to the source.

Registry Subkey Value Encryption:

Registry values in many places under the subkeys are weakly encrypted using "ROT-13" algorithm which basically substitutes a character with another character 13 position away from it in the ASCII table.

Even though each registry value is not associated with specific time and date the event occurred, it could imply suspect has accessed certain file or object.

How to make sure the evidence we have extracted is admissible:

- Save the exported key contains evidence in a external device (preferably read only saving) and make sure there is not any code or program changing this evidence derived. To do so we have to take a look to the programs installed in the key is for all installed programs (in following pages is explained).
- Include the date and time with the evidence we are exporting in a text file.
- If above instructures are not available for us in any reason take a picture of current registry key is open and save it in a external device including date and time.
- Before starting any evidence investigation take a picture of computer status from hardware and software screen situation before any launch.
- One of the strong evidences is making sure there is a hacking tool on system which preserves the main chain of custody by its relation to another evidence which is hackers IP or Mac address can be found in registry keys and the current IP/Mac address.

Hackers Unauthorized Access to Registry Keys:

By proving the unauthorized access to Registry keys and relating such access to an external address or his fingerprints indicates a hackers unauthorized access. Since attaching and installing any software or execution code needs administrators privilege any one attempt to install a code must be an administrator and in Windows XP and Vista system has extra awareness to make sure about it. Specially in Windows Vista before every access and install the system refers the user to get permission and make sure he has the permission to go further. So generally hackers cheat the users to install their program under the user's name and then continue monitoring or treating with victims. These codes are being installed under advertisement or some useful tool coverage to spoof the users. To find out the hackers we need to find their address either Dynamic or Static to relate them to the system corruption. Through the keys defined below based on the address type we can find the computers that had access to the system.

How to find out there is botnet installed on computer:

A bot is a compromised computer which is running software that allows a remote computer to control it. The software is usually installed by someone breaking into the computer, but can also be installed by a user who thinks they're installing a game or other software which they have downloaded from a website or received via Instant Messenger (IM).

A botnet is a large collection of compromised computers (bots) which are controlled by a very small number of remote computers. Communication is often done using Internet Relay Chat (IRC, an older instant messaging protocol).

Botnets are often used to send spam (both E-mail and IM), compromise other computers, and launch distributed denial of service (DDOS) attacks. In some cases, DDOS attacks

are used to threaten commercial entities, or even damage their online websites by flooding them with a large amount of traffic.

Type of bots:

- DDOS (Denial-of-service) attacks where multiple systems autonomously access a single Internet system or service in a way that appears legitimate, but much more frequently than normal use and cause the system to become busy.
 - Adware exists to advertise some commercial entity actively and without the user's permission or awareness.
 - Spyware is software which sends information to its creators about a user's activities.
- E-mail spam are e-mail messages disguised as messages from people, but are either advertising, annoying, or malicious in nature.

Advertiser Bot Removal Instructions:

- To stop all Advertiser Bot processes, press CTRL+ALT+DELETE to open the Windows Task Manager. Click on the "**Processes**" tab, search for Advertiser Bot, then right-click it and select "**End Process**" key.
- To delete Advertiser Bot registry keys, open the Windows Registry Editor by clicking on the Windows "**Start**" button and selecting "**Run.**" Type "**regedit**" into the box and click "**OK.**"
- Once the Registry Editor is open, search for the registry key "**HKEY_LOCAL_MACHINE\Software\Advertiser Bot.**" Right-click this registry key and select "Delete."
- Finally, to completely get rid of Advertiser Bot, we must manually remove other Advertiser Bot files. These Advertiser Bot files can be in the form of EXE, DLL, LSP, TOOLBAR, BROWSER HIJACK, and/or BROWSER PLUGIN. For example, Advertiser Bot might create a file like

%PROGRAM_FILES%\Advertiser Bot\Advertiser Bot.exe. Locate and remove these files.

DDoS Bots removal instruction:

All types of bots use a technique which enables them to hide from normal task list.

- Disable the “hide files” option within windows. To do this, open windows explorer, choose tools, folder options, view and instruct windows to show all files. Also disable the hiding of file extensions and the hiding of system files as both of these can disguise the location of DDoS bot files.
- Search all the files and folders for a file called mirc.ini. If this file is found anywhere other than in our mIRC directory, it’s probable that there is a bot installed in that directory. There should never be a mirc.ini file in the system directory or any subdirectory of it - if we find one there it’s almost certain there’s a hidden bot installed on the machine.
- Check for running processes that cannot be recognized. To do this, we will need to shut down all programs and disconnect from internet. We should then run the Microsoft system information utility (C:\Program Files\Common Files\Microsoft Shared\MSInfo\MSinfo32.exe). Once open, we need to select Running Task from the list to the list of option under software environment. This will show us lists of tasks are running on machine. Compare this list to the one found under Startup Programs. Anything found in both lists is worth a closer look. We must check for files we don’t recognize or which seem to be in unusual places or which we don’t think should be running automatically when we restart the machine.
- We must check for the registry keys for startup programs we don’t recognize.

The keys are:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

OR

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

OR

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

- The most common filenames can be found are as below:

WHVLXD.EXE

Temp.exe

Temp2.exe

Accessdriver.exe

pepsi.exe

SETUP.EXE

Anti_Net_Bus.exe

setting.exe

DskLoad.exe

vscan2001.exe

expl32.exe

explorer2.exe

BLuESpYdER.exe

lgmp.exe

mimic.exe

win32.exe

reg.exe

something.exe

speedup.exe

xxvideo.exe

sex.exe

winini32.exe

nohack.exe
bot.exe
temp.scr
Animal.scr
BRITNEYSPEAR.scr
BRITNEYSPEARS.SCR

The key investigation from registry platform are categorized in four chapter as below
(refer to Appendix A)

Hardware:

To Find Current Hardware Profile Configurations:

The system key:

In general HKEY_CURRENT_CONFIG is a symbolic link to current hardware profile configurations subkey, HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current. Current is a link to the key HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\XXXX.

To Find per Computer Setting:

Every computer has the specific setting stored in key which can be useful. This key contains the whole setting about the computer in general with more detail on following pages.

The System key:

HKEY_LOCAL_MACHINE, totally Contains computer-specific settings which apply to all users logging into that particular computer.

HKEY_LOCAL_MACHINE Subkeys:

some general information before going to detail:

- **Subkey: HARDWARE-** Stores information regarding hardware Windows XP detects during startup. They include information on device driver and associated resources.
- **Subkey: SAM-** Security Accounts Manager (SAM) is a local security database which contains local users and groups information. ACL prevents Administrator from viewing this subkey.
- **Subkey: SECURITY-** Contains Windows local security database in the SAM subkey. ACL prevents Administrator from viewing this subkey.
- **Subkey: SOFTWARE-** Stores per-computer application settings. Programs store their settings in this standard form, HKLM\Software\Vendor\Program\Version.
- **Subkey: SYSTEM-** Contains control set, which contains device driver and service configurations. HKLM\SYSTEM\CurrentControlSet is a symbolic link to ControlSetXXX, and the key HKLM\SYSTEM\Select indicates which ControlSetXXX is in use.

To Find Most Recently Used Network Printers:

The shared printers which are available through network being stored in registry keys and most used shared printer

The System key:

HKCU\Printers\Settings\Wizard\ConnrctMRU

This key contains the information regarding most recently used network printers by user. Depending to the number of existed software the number of subkeys will be indicated.

The system key:

HKCU\Printers\Settings\Wizard\ConnrctMRU\DevModperuser contain the names of software has developed the printer to their configurations.

To See List of Mounted Devices:

Mounted devices are devices are installed by computer and the information are saved.

The system key:

HKLM\SYSTEM\MountedDevices

This key contains a list of mounted devices, with associated persistent volume name and unique internal identifier for respective devices.

For instance, if the binary data for registry value "\DosDevices\F" contains "\"??\Storage#RemoveableMedia" at the beginning of the value, it signifies a USB removable disk was connected to the system USB port. By correlating the entry with registry key LastWrite time, investigator would know when the removable device is connected.

To Get More Information on the Device:

The key below mostly represents the devices are installed on computer base on their Number and the numbers must be transfer to the readable information.

The system key:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\

Contains information which is located under the respective device GUID (Globally Unique Identifiers) subkey and in the binary registry value named Data

To Find Addition Information about List of Mounted USB Storage Devices:

On this key below the more information about the USB device like hardware ID, Device description and its class can be find.

The system key:

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR

This key Contains addition information about list of mounted USB storage devices including external memory cards

USB storage device unique serial number can be acquired via UVCView program, under the field "iSerialNumber".

This key will have a subkey containing device name, such as "Disk&Ven _USB _Card&Prod _IntelligentStick&Rev _1.00 ".

Under this subkey is the device ID subkey which contains the device serial number; "20000101061325-00&0". The latter subkey has a ParentIdPrefix value (data="7&1064d032&0") which corresponds to the binary registry value in

HKLM \System\MountedDevices; \DosDevices\F for instance

The latter value will contain binary data similar to "\\?\Storage#RemoveableMedia#7&1064d032&0". By mapping this two key, forensic examiner will know which USB device (using device serial number) is mounted to which drive letter. Apple iPod devices leave similar trace.

Software:

To Know Software Setting for the Local Machine:

In general the key below contains the information of setting for Local Machine.

System key HKLM\SOFTWARE.

This key mainly contains the information about software setting on system. We will discuss about details in following pages.

Software Setting that is Users Specific:

On this part mainly the software information that is configured by user will be shown.

We will discuss about the exact evidentiary data on this key later.

System key HKCU\SOFTWARE.

The Installed Applications Path and Execution Address List:

The first location to look at is the root of the software key itself. Program located here may be obvious by their name, or they may be more obscure, being listed under an innocuous or even bogus company name. Often these bogus names are obvious when we see them, but we have to look to find them.

System key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App paths

On this part we can find the programs are installed on system with their path which the execution file is exist there. Existence of any suspicious tool or its path on this part is considered as evidence.

Other location to examine for software is the following two registry keys:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\currentVersion\Uninstall

To Know Uninstalled Program List:

Software are often installs an "uninstall" key that provides information for program removal.

The System key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\currentVersion\Uninstall

This key contains a list of subkeys that each of them correspond an uninstalled program with the specific user information and data and time program uninstalled. By clicking on each key we can have a look to uninstalled address, source, and the publisher name and of course if there a malicious program it will be embedded on this section.

To Get SID User Profile List:

The system key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList

This key provides a listing of Subkeys, each named after SIDs on the system. If a user has interactively logged on to the machine, using a local or domain account, there will be a Subkey with that user's SID for its name. There is a value for that Subkey named ProfileImagePath. The string data for this value will list the path to the user's profile.

To Find Stored Restore Points:

The system key:

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWSNT\CurrentVersion\SystemRestore stores restore points in the registry and the “LastRestoreID” Value name is the id for last one has restored the system can be resolve by a tool. So the ID would be considering as evidence.

System Key HKEY_CLASSES_ROOT:

This key is from merging two keys:

- 1- HKLM\SOFTWARE\Classes (contains default file associations and class registration) and
- 2- HKCU\Software\Classes (contains per-user file associations and class registration) and consist of file types, filename extensions, URL protocol prefixes and registered classes, protocol prefixes and registered classes.

The actions defined here tell Windows how to react to every file type available on the system.

To Find Disabled MRU Files in Registry:

The MRu files are most recently used files.

System key HKEY_CURRENT_USER\ Software\Microsoft\ Windows\ CurrentVersion \Policies\Comdlg32 key

If there is a value with strange name with value of 1 is for setting the MRU or most recently used files off or making them disable.

The Order of Listing MRU Files:

The system key:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

This key describes the order as string of those lettered value names with most recent being listed first and the oldest at last. For example if the data value of the MRU list is “a” that means sorting MRU files will be listing from a to z.

To Find Recent Search Terms:

The system key:

HKCU \Software\Microsoft\Search Assistant\ACMrU

Contains recent search terms using windows default search, Subkey 5603 contain search terms for finding folders and filenames, while subkey 5604 contain search terms for finding words or phrases in a file.

To Know Autorun File on Registry:

The system key:

HKLM\SOFTWARE\Microsoft\Command Processor

Contains a registry value named Autorun, which could contain command that is automatically executed each time cmd.exe is run. Malware exploits this feature to load itself without user's knowledge.

To Find Windows Protected Storage:

The system key:

HKCU\Software\Microsoft\Protected Storage System Provider

Contains Windows Protected Storage. Protected Storage is a service used by Microsoft products to provide a secure area to store private information. Information

that could be stored in Protected Storage includes MSN Explorer and Internet Explorer AutoComplete strings and passwords, Microsoft Outlook and Outlook Express accounts' passwords, and MSN Messenger password. Registry Editor hides these registry keys from users viewing, including administrator. There are tools that allow examiner to view the decrypted Protected Storage on a live system, such as Protected Storage Pass View.

IP Address Interfaces:

There is various interface configurations for IP addresses that have been configured on the machine. They will exist for either static (fixed or assigned by the network administrator) or dynamic (assigned on the fly by a DHCP).

The system key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces;

If enabled DHCP is set to zero, meaning that dynamically assigned IP address are not being assigned. The IP address value shows the fixed IP address.

The default Gateway value describes the Gateway router for this configuration.

To Know the Last Logged On Users:

The system key

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

Indicates the setting for showing the last logged on user so if the string value DontDisplayLastUserName set for 0 there won't be last logon show for user.

To Find the Disabled Default Administrator Shares:

The system key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters, indicates this option and when Windows NT has several hidden shares

that can only be accessed by an administrator. The hackers Change the REG_DWORD value AutoShareServer Type from 1 to 0 to disable the default administrative shares.

To Enable Custom Logon Message:

The system key:

HKLM\SOFTWARE\Microsoft\ WindowsNT\CurrentVersion\Winlogon,

key is for create a custom Logon message as display a legal notice that will be displayed during logon and users will be forced acknowledge the message by selecting ok prior to logging on.

Create a String value named LegalNoticeCaption and enter the text that will be the caption for the message. Create a String value named LegalNoticeText and enter the text of the message.

To Find the Changed Default Name and Company Information:

The user key:

HKEY_CURRENT_USER\Software\Microsoft\MS Setup (ACME)\User Info contains this information, to change these parameter we need to Modify the two values named 'DefName' and 'DefCompany', and change the values to our current Name and Company respectively. And to find the changed parameters we need to compare the time stamp for this value with the windows installation time stamp.

Proxy Server Configuration Values:

The user key:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\

Internet Settings;

The values that configure the Internet proxy setup are located in this key. To find which proxy server is used, take a look the value of 'ProxyServer' to equal the server and port combination. For example if the proxy server was called \PROXY and it was

running on port 80 then the setting would equal 'PROXY: 80'. We may also need to have a look to the value if 'ProxyEnable' to equal '1' the proxy is enabled or '0' is disabled. Setting the value of 'ProxyOverride' to equal '<local>' will stop internal addresses from going through the proxy.

Network:

To Find System IP Address and Default Gateway:

The system key:

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID

This key contains network adapter recent settings such as system IP address and default gateway for the respective network adapters. Each GUID subkey refers to a network adapter.

To Find Wireless Network Information:

System key:

HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\GUID

Contains wireless network information for adapter using Windows Wireless Zero Configuration Service. Under the GUID subkey, there are binary Registry values named Static#0000, Static#0001 which correspond to the respective list of SSID in “Preferred Networks” box in Wireless Network Connection configuration.

If suspect connect to wireless networks using other 3rd party program that is usually bundled with the network adapter, instead of using Wireless Zero Configuration, no trace is left on this key.

Forensic examiner can use this key with the previous network adapter GUID key to determine the last assigned IP address.

Mapped Network Drive, Server Name and Shared Folder:

System key:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MapNetwork Drive MRU.

Maintains a list of mapped network Drive, including the server name and shared folder the value in this key is still retained even though the mapped network drive has been permanently removed or disconnected.

And the key:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2, is the Permanent subkey regarding mapped network drive is also created in the second key, and the subkey is named in the form of ##servername#sharedfolder.

Windows:**Main per User Information key:**

System key:

HKEY_USER

Contains subkeys that each of them refers to certain user identity which is recognized by SID numbers. The secondary user SID (usually administrative account SID) will only present in the HKU sub keys if the user performs a secondary logon during the user's session. If an offender performs a secondary logon on any other accounts, the secondary user sub key will exist in HKU until secondary user logoff, or the program running in the elevated privileged is closed. For more investigation information or exact SID number extraction we need to refer to a tool.

- **User Basis Stored Data for Application Key:** HKEY_CURRENT_USER
- **Local System Account Identity:** HKEY_USER\S-1-5-18
- **Local Service Account Identity:**
System key: HKEY_USER\S-1-5-19.
It is used to run local services that do not require Local System account.
- **Network Service Account:**
System key: HKEY_USER\S-1-5-20.
It is used to run network services that do not require Local System account.
- **First Logon on Computer:**
System key: HKEY_USER\S-1-5-21.
Refer to the main user first logon on computer and first account making.

Microsoft Outlook Express Identity:

Subkey:

HKEY_CURRENT_USER\ ENVIRONMENT

Corresponds to an identity in Microsoft Outlook Express,

Subkey:

HKEY_CURRENT_USER\IDENTITIES

Corresponds to the identities in Microsoft outlook express since Outlook Express allows multiples identities (users) to use a single mail client.

Mapped Drive Windows During User System Logon:

Sub key:

HKEY_CURRENT_USER\NETWORK,

Each Network subkey corresponds to a mapped drive Windows connects during user system logon. Subkey name is the drive letter to which the network drive is mapped. The subkey contains configuration to connect the network drive.

User-Specific Application Settings:

The sub key:

HKEY_CURRENT_USER\ SOFTWARE,

Contains user-specific application settings, Programs store their settings in a standard way, HKCU\Software\Vendor\Program\Version\, Vendor is program's publisher; Program is the Program's name; and Version is program's version.

Environmental Variables:

The sub key:

HKEY_CURRENT_USER\VOLATILE ENVIRONMENT,

Contains environmental variables that are defined when user logon to Windows XP.

Last Visited MRU Lists Program:

The system key:

HKCU\Software\Microsoft\Windows\Currentversion\Explorer\ComDlg32,

Contains Last visited MRU lists program and the files opened by them. To see their names we can export them in a text file through File-Export Menu and have a look to their filtered name in text file. For more information extraction we need to use investigation tool.

Most Recent File Opened and Saved:

The system key:

HKCU\Software\Microsoft\Windows\Currentversion\Explorer\ComDlg32\OpenSave MRU,

Lists the most recent files opened and saved, grouped by extension;

Files or Words Search Phrases:

System key:

HKCU\Software\Microsoft\Windows\searchAssistant\ACMru

Contained of user/intruder searches for local or networked drives for files/directories or words/ phrases.

User Name of Last Log On:

The system key:

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ Winlogon

The value name DefaultUserName stores the username of the last-logged-on user so that it can be displayed as the default username for the next logon.

Permitted Terminal Services Connections:

System Key:

HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\TERMINAL SERVER.

There is a value in this key named fDenyTSConnections. If we enable remote desktop, its value will be 0, meaning the terminal services connections are not being denied, meaning they are being permitted.

To Know Systems Time Zone Information:

System Key:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation

Contains time zone information, including the difference in minutes between UTC and local time, and reference information during daylight saving time. When the value “TimeZoneKeyName” is containing current time zone system is set on it. so by

comparing value key time zone we can make sure about the time this time zone has changed or set.

Most Recently Used Files:

System Key:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU. Maintains list of recently opened or saved files via typical Windows Explorer-style common dialog boxes. Subkey * contains the full file path to the 10 most recently opened/saved files. Other subkeys in OpenSaveMRU contain far more entries related to previously opened or saved files (including the 10 most recent ones), which are grouped accordingly to file extension. But for the clear filtering we will need to have a tool.

List of Recently Executed Files:

System Key:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs.

Maintains list of files recently executed or opened through Windows Explorer. This key corresponds to %USERPROFILE%\Recent (My Recent Documents).

The key contains local or network files that are recently opened and only the filename in binary form is stored. The Subkey Folder contains the folder of the recently open files. Subkey NetHood which corresponds to %USERPROFILE%\NetHood contains only LAN shared folder path which the file was opened. We need a tool to filter the binary data for extraction.

Executed Files Using the Start>Run Commands:

System Key:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Maintains a list of entries (e.g. full file path or commands like cmd, regedit, compmgmt.msc) executed using the Start>Run commands. Most recently added entry

does not imply most recently used command. To filter binary data we need a conversion tool.

To Find Uninstalled Program:

System Key:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall.

Each subkey in this key represents uninstalled program in the computer. All programs listed in Control Panel>Add/Remove Programs correspond to one of the listed subkeys.

Automatically Programs Running Path:

System Key:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

System Key:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

System Key:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce

Usually contain programs or components paths that are automatically run during system startup without requiring user interaction. Malware usually leaves trace in this key to be persistent whenever system reboots. Subsequent four subkeys may also contain suspicious entries. Similar 5 sets of "Run" registry keys may exist under root key HKCU, pertaining to the logged on user configuration. The program HelpLink, Help Telephone, Install Location, Install source, Publisher Name, URL Info About, URL Update Info is available from Value Data.

Windows Services List:

The System Key:

HKLM\SYSTEM\CurrentControlSet\Services

Contains list of Windows services, each subkey represents a service and contains service's information such as startup configuration and executable image path. Some

malware such as BackOrifice2K will install itself as service. Thus, it leaves trace in this key. So if we are suspected to a malware we must have a look to this list and find the suspicious services. To do so we must be familiar to usual windows services.

To Find Instruction to Execute .exe Extension Files:

The System Key:

HKCR\exefile\shell\open\command

This key contains instruction to execute any .exe extension file. Normally, this key contains one default value with data “%1“%*. However, if the value's data is changed to something similar to somefilename.exe "%1" %*, investigator should suspect some other hidden program is invoked automatically when the actual .exe file is executed. Malware normally modify this value to load itself covertly .This technique applies to other similar keys, including:

HKEY_CLASSES_ROOT\batfile\shell\open\command

HKEY_CLASSES_ROOT\comfile\shell\open\command

To Find File Execution under Right Click Command in Windows:

System Key:

HKCR\Drive\shell\ and HKCR\Folder\shell\.

These two key contains subkeys that refer to menu items in Windows context menu. The first key points to the context menu when right clicking on Windows drive letter, while the second key refers to folder's context menu.

By modifying the default registry Value's data to cmd.exe /k "cd %L" && start Notepad.exe, the two programs are launched separated under different windows. Thus, the second program can be loaded covertly. This technique applies to other similar keys, including:

HKEY_CLASSES_ROOT\batfile\shell\open\command

HKEY_CLASSES_ROOT\comfile\shell\open\command

System Objects and GUID Subkeys:

System Key:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist.

Contains two GUID subkeys, Each subkey maintains a list of system objects such as program, shortcut, and control panel applets that a user has accessed.

The GUID subkey beginning with "5E6" corresponds to IE toolbar, while subkey starting with "750" pertains to Active Desktop.

Security:

To know the Source Cause Restricted Access to the Contents of Selected Drives:

The System Key:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

The "NoViewOnDrive" value uses a 32-bit bitmask to define local and network drive access for each logical drive in the computer. The lower 26 bits of the 32-bit word correspond to drive letters A through Z. Drives are visible when set to 0 and hidden when set to 1.

To Find Specific Applications Restricted From Running:

The System Key:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

To do so we must create a new DWORD value and name it "DisallowRun" set the value to "1" to enable application restrictions or "0" to allow all applications to run.

Then create a new sub-key called

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun]

And define the applications are to be restricted. Creating a new string value for each application, named as consecutive numbers, and setting the value to the filename to be restricted (e.g. "regedit.exe"). Also existence of such values corresponds the restriction of application which can be considered as evidence.

To Find a Disabled Run Command from Registry:

The System Key:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer].

Value Names: DisableLocalMachineRun, DisableLocalMachineRunOnce, DisableCurrentUserRun.

Created a DWORD value for each of the optional values which is indicated over here is depended on which Run function to stop. The value must be set to "1" to disable the application. So to find them we need find these values with the optional value when it is set to "1".

To Find the Restricted Access to Windows Updated:

the windows updates will download and install the latest patches to protect the system from latest flows and problems has discovered by Microsoft specialists and restricting them from being updated cause system to stay in unstable conditions which can be a benefit for intruders.

System Key:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

Created a DWORD value named "NoWindowsUpdate" and the value set to equal "1" makes this work to be completed.

This restriction may also be enforced by using the "DisableWindowsUpdateAccess" DWORD value in the

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WindowsUpdate] key.

To Find the Reason Why Registry Editing Tools are Disabled:

Some of the tools like registry cleaners need to change the registry values to the default value in order to solve the problems but there is an option can make the registry not writeable by tools.

User Key:

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

And the DWORD value named 'DisableRegistryTools' with set the value to '1' to disable registry editing functions. This can also be enabled on a user-by-user basis by putting the same value in the [HKEY_CURRENT_USER] hive.

The Hidden Drives in My Computer:

Sometimes there is no device we can see in my computer, at this time maybe we think there is problem with windows or executed any Virus which may cause us to get confused in our thinking. But there is another probability which is the devices has been made hidden through registry keys.

System Key:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

The "NoDrives" value uses a 32-bit word to define local and network drive visibility for each logical drive in the computer. The lower 26 bits of the 32-bit word correspond to drive letters A through Z. Drives are visible when set to 0 and hidden when set to 1.

Disables Shutdown Command:

Another issue we may face is disabled or disappeared shutdown command from start menu. This command has an option which can be disabled through Registry.

System Key:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies
 \ Explorer]

Created a DWORD value, or modified the existing value, called "NoClose" and set it according to the value data "1" for disabled and "0" for enabled.

Disable Menu Bars and the Start Button:

The System Key:

[HKEY_CLASSES_ROOT\CLSID\ {5b4dae26-b807-11d0-9815-00c04fd91972}]

Represents this option with renaming the key by placing a dash "-" in front of the GUID (for example {-5b4dae26-b807-11d0-9815-00c04fd91972}).

Hidden Control Panel, Printer and Network Settings:

System Key:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies
 \ Explorer]

the existence of a new DWORD value, or modified existed value called 'NoSetFolders' with data value "1" for enabled and "0" for disabled.

Disabled User Tracking:

This setting stops Windows from recording user tracking information including which applications a user runs and which files and documents are being accessed.

System Key:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies
 \ Explorer]

To make sure about it there should be created DWORD value named "NoInstrumentation" and set the value equal to "1" for enabled restriction.

Cleared Internet Explorer Typed Address History from Registry:

Internet Explorer caches any URLs that are typed into the address bar. This may become a privacy issue on a shared computer, or maybe there is a particular address has been removed.

User Key: [HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs]

Any value can be deleted or the entire key maybe deleted to delete all entries. This evidence is more reliable with using a forensic tool, because on such tool we can see all the deleted entries. Or we can rely to the last date and time this key has been touched but this is not enough we have to stick the time stamp to another evidence to make it beyond reasonable doubt.

4.4.2 Windows XP and Vista Registry Forensic Guideline Via EnCase Investigation Tool:

- 1- First Step Create a Case.** Click on the “new” button in case view section. At this stage enter the name, examiner name, default export folder and temporary folder.
- 2- Include the Sub Files in Search** by click on the “set included folder” trigger sign from tree pane view in case view part.
 - a. To Have the live Device Investigation** the blue triangle in lower right of physical device should be visible as live device in tree view part.
 - b. To Set Certain Columns Visible** in table view pane during the process of investigation set the columns locked by right click on them and choosing the “set lock” option from column field.
 - c. To Choose Which Columns are Visible** right click on the table view and choose need columns by clicking on show columns.

- 3- String Search on Encase** is consisting of adding keywords and choosing file/folder to search on. Registry files are considered as logical evidence which can be created from existing evidence files which is implication of logical search implementation.
- 4- View the Registry Information**
- a. Through built in registry viewer
 - b. Find the correspondence file in windows, usually in “SAM” and “Config” folder contain Security, System and software files (Windows XP)
 - c. Find the registry files from System32\Config\RegBack\Security (Windows Vista)
- 5- Live Windows Registry Evidences** are consideration of auto run keys, devices, installed software, build information, networking details, user information and hardware details and registry hives when windows is running.
- 6- Hardware Analysis,** Encase culls hardware information automatically through registry and configurations to identify the types of hardware installed or previously installed on target machine. The devices like: IDE, USB, and FireWire.
- 7- Find Evidences in Chronological Activity** is available through timeline tab. Each tiny red square represents a file, and placing our cursor on it displays its context in view pane. Square’s color are represented below:
- **Dark green:** Created file
 - **Green:** Written file
 - **Light Blue:** Accessed file
 - **Dark blue:** Modified

- **Red:** Deleted file
- **Black:** Log off

8- Registry Browsing will be available in Encase by exploring in table pane and find them through correspondence file in windows. . In Windows XP the registry keys usually can be finding in SAM folder which contains Security, System and software files. These files are stored in

C:\%SYSTEMROOT%\system32\config\ Registry keys are in files by .DBB and .DAT extensions.

And In Windows Vista the registry keys are in path below:

C:\Windows\System32\config\RegBack\SECURITY.

9- Registry Analyze as a Compound File, in Encase is implemented by viewing the individual components of compound files within an evidence file and to view their structure there is need to making them as evidence by bookmark option from right click on the selected data. That means at the first we need to make a bookmark from the data we have selected then mount them as an evidence to have a look to the structure by clicking on “view file structure”.

- Compound files are typically files that are comprised of multiple “layers” such as registry files. Registry files on NTRegistry or NTuser are considered as compound file that we can see their structure by selecting “view file structure” on the text overview file structure.

10- SID Numbers Extraction from Registry Keys; To know the detail about SID numbers we need to filter the text as we can see on the view pane, So at the first we have to find the SID number then select the hex text part from view pane and bookmark them, after choosing the bookmark we can select the filter we want to view these texts with it which can be Date and Time format, windows info file record or other formats. Encase extracts the owner, group and permission setting on windows systems.

11-To Get Software Disk Configuration, Encase virtually mounts the software disk configuration within the Encase case. Also Encase reads the Dynamic Disk partition structure and resolves the configurations based on the information extracted. To rebuild a dynamic disk configuration, add the physical devices involved in the set to the case and from the Cases tab, right on any one of the devices and choose Scan Disk Configuration.

12-Make Report of What Has Been Obtained; after mounting the evidences through Encase Investigation tool the Encase has ability to make a report by the adjustment information and column in it So the presentation of the evidences are more accurate and stable and more trustful because the Encase has the standard to be accepted in legal forms as a formal investigation forensic tool.

13- Filters; work with filters is very simple and easy and actually the Encase has made everything very simple than data acquisition from manual way. So on the filter section there are some functions can be executed and acquire the information we want in the form of filter we choose. For example Security ID groups, Security ID names or dates, Registry keys or deleted folders. The only thing we need is to run the filter by double click on them and make a report of what we have found in case there are evidences.

14- Query; one of other available options can help is the queries which are doing slightly same job with filters but the different between them is Queries are editable and we can mix two, tree queries together to get different result.

Chapter 5

Discussion

5.1 Introduction

After having all experiment to produce windows registry guideline some of the problems which are related to registry platform of windows XP and Vista guideline preparation and they have the value to be cited on this chapter will be discussed here.

Also in regard to protect windows registry by the ways we have indicated on guideline chapter there are some criteria that need to be considered to choose a proper registry cleaner tools.

The survey of having study in different articles in literature review and their point of view comparing with this guideline ideas are also being considered in following sections.

And also the influence and usability and the performance of this guideline on defined users and scope has been surveyed in following pages.

5.2 Performance of windows XP and Vista Guideline

The main points regarding the guideline performance are listed below:

- This guideline makes the users more comfortable to work with registry, because of its separated steps help the users to have meaning full review of this area in form of investigation.
- The registry environment is a complex area in many users idea and so in producing of this guideline we have tried to make the users out of confusion.
- Based on the performance measurement of this study the higher performance is for the ones had a review of registry area before.
- Comparing the two guidelines we have prepared based on straight keys and the Encase tool; the users investigating with the tool have found the investigation work is easier for them by this guideline.
- Saving time and not involve to technical parts are the points real inspectors want from investigation job when they had the technical experiment to use in necessary situations, so about 75 percent of them would like to investigate with Encase and just for some situations refer to straight looking evidences.

5.2.1 Influence of Windows XP and Vista Guideline on Defined Users

Since the registry keys can attract a few ones to study on it, having “a streamline paper to follow” seems necessary for investigators. Specially now a days working with tools help a lot to make the time shorter and the performance higher than it is without using tools, so of course the performance of investigation with Encase tool in our

experience is higher. But the point for straight key searching guideline is that some of the investigators in any situation may don't have a tool so this issue should not make them unable of investigating which is because of relying more to the tools and digital world.

5.2.2 Guideline Usability Statement between Different Users

The different users defined in scope of this project have the different experience in their job which is mainly digital investigation and in this statement we have divided our users to 3 main batch based on the experience time they have to get the result of how many of them are more interested to which kind of investigation base on two type guideline we have prepared. The statement is as below:

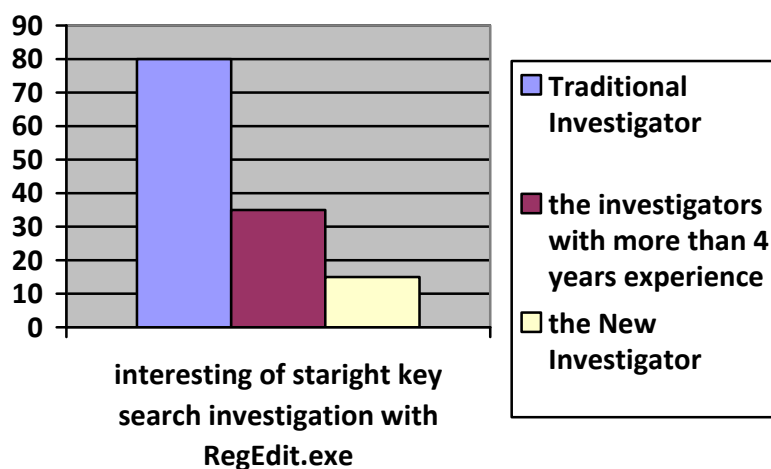


Figure 5.5.1: Interest of using Regedit.exe

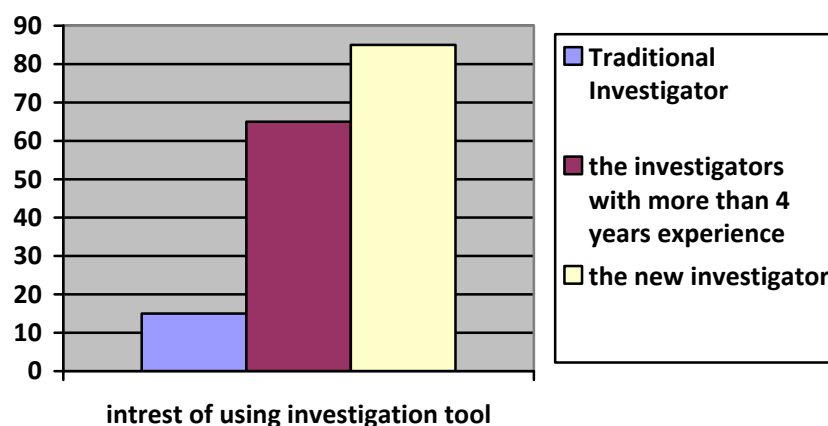


Figure 5.5.2: Interest of Using Encase

5.3 The Literature Review and Conclusion

Before starting to come out with the guideline on the literature review we had a review plenty of articles about Registry Environment, Registry Keys, Registry Hacking, and Registry Weaknesses and so on, until we found there cannot be find a guideline regarding registry investigation with particular users and windows versions we have defined in audience section. It was in a situation many of them speak about these keys and how they can be useful, except the Encase tool that is came out with a complete structure of having investigation but this tool too still did not have investigation guideline with such users and in defined windows versions.

5.4 Hidden Information in Registry Entries

There are some evidences cannot be found during Investigation with currently produced guideline. By the time we had experience to choose the right keys of forensic guideline there are some places that the evidences can be hided without inspectors knowing where the place of evidence is.

Suspect can hide all sorts of data including password, text information, and binary files in registry. Suspect can effectively hide data in registry keys value entries. By using different encoding techniques, suspect can obfuscate or hide data from forensic examiner.

The flaw involves any registry values with name from 256 to 259 (maximum value name) characters long. The overly long registry value (regardless of type) not only hides its own presence, but also subsequently created values (regardless of type) in the same key. The editor stops displaying the remaining of the values thinking the overly long value as the last value in that key. Suspect can exploit such Registry Editor flaw to hide information.

Since registry's value supports binary data type, suspect can store segments of program or the entire binary in the registry. These segments of program can be placed in several dispersed keys. Unless forensic examiner knows the relevant keywords to search in the registry, finding hiding data in tens of thousands of registry keys can be a tedious task.

An example of a place to hide data is in the time zone information key, `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation`. This key contains time zone information, including the difference in minutes between UTC and local time, and reference information during daylight saving time. Windows

reads this registry key into `TIME_ZONE_INFORMATION` structure during system startup.

There are two strings in `TIME_ZONE_INFORMATION` structure, `StandardName` and `DaylightName`, of which can legally be an empty string. Any information written to them using `SetTimeZoneInformation()` function is returned unchanged by the `GetTimeZoneInformation()` function. Since, and they are merely used for storing string information, suspect can hide information such as passwords or passphrases in these values effectively. Suspect merely modifies registry values `StandardName` and `DaylightName` manually using Registry Editor to store information. Suspect can retrieve this information using a piece of code by calling `GetTimeZoneInformation()` function which is loaded in Windows `kernel32.dll` without raising much suspicion.

5.5 Time

There is a shortcoming in Registry environment during the experiment we had in working with registry of windows which is the time and date the event occurred whereas it is not associated in each registry values, it could imply suspect has accessed certain file or object. Even though we can export the last date and time the key has accessed but not the value.

5.6 Registry Cleaners

Since the protection of registry environment is one of main parts to preserve the windows Configuration repository, the Registry cleaners help a lot to find, analyze and clean the keys from being in any danger and finally protect the whole system.

Here are the listed complete features that a registry cleaner tool should have to be considered as a complete tool for registry cleaning. Here is some information based on the results of tests and analysis of Registry Cleaner sites as below:

Features:

- Live On Guard Protection
- Pop Up BLOCKER
- Spyware Remover
- Adware Remover
- BHO Manager
- Immunizer
- Descriptions of Problems
- Deep Scan
- Scanning Log
- Ignore Lists
- Back Up/Restore
- Startup Manager
- Registry Optimizer
- Registry Compactor

Detect and Repair

- Application Paths
- Shared Program Paths
- File Associations
- Active X Controls
- Add/Remove Programs
- Help Files
- Font Files
- Toolbars
- Shared DLL Files
- Invalid Shortcuts
- Startup Files
- Most Recent Files
- Shared DLL Files

Technical support

- Email
- Application Help File
- Scan Log Analysis
- Live Web Based Support
- Knowledge Base FAQ's

Operating software supported

- The five most up-to-date operating systems

A full registry scanner to clean:

- Automatic/Manual Removal
- Shows scan progress
- Back-up Registry

- Built in scheduler
- Compress or Defrag Registry
- Manage/Cleanup Startup Programs
- Scans for Invalid Program shortcuts
- Removes Duplicate files
- Deletes empty registry Keys
- Checks invalid Class Keys
- Checks Shell Extension
- Checks invalid Help Files
- Checks Invalid CLSID/Typelib/Interface Entries
- Checks Invalid Shared known DLL's
- Checks invalid Paths
- Checks Application Path Keys/Orphan References
- Checks Invalid Fonts
- Checks Invalid File Types//Extensions/Entries
- Startup manager

Chapter 6

Summary and Future Work

In this chapter, a summary of the design and operation applied in this research was presented. The total experiment summary will be discussed and follow it up with some recommendations for future work to improve the security and overall investigation performance.

6.1 Summary

Windows registry is an excellent source for potential evidential data. Knowing the type of information that could possible exist in registry and location to it gives forensic examiner the edge in the forensic analysis process. Investigator will get a better picture of the whole case. The fact that Microsoft and other organizations treat the registry settings as in-house information without providing sufficient and comprehensive

documentation about the registry keys used causes registry analysis difficult, which undermines the resourcefulness of registry. Thus, there is a need to unveil and publish evidentiary registry keys to assist forensic investigation on Windows system.

The experiment and study used to identify the windows XP and Vista registry platform by analyze the important features, the tools and tested approaches to find out what kind of useful information the registry can bring for a user either has or doesn't have the technical background of it.

Even though the short comings are not important on this study as is going to produce a guideline but we have experiment some flaws on this study during the testing, working and studying. These limitations and information leakage on windows registry makes hackers job easier and forces some investigators to develop complicated tools to cover these shortages although these tools are quiet helpful to bringing the strong evidences as long as they are not available on windows. Therefore registry of the windows needs to have a complete analysis to improve the investigation of the information on this scope so there need to be solutions for exploited flows of the registry as well. The flaws have mentioned on discussion chapter which need to be covered with windows security patches and new configuring of registry platforms.

The main experiment of this project is to highlight the registry evidences for the users who don't have the background information and technical knowledge and the ones who have the Encase investigation tool to go further more in it. So the produced guide line is as a comprehensive guideline which is completely new forensic world.

6.2 Further Work

Searching for information in Encase tool has been proven to be good and accurate software by NIST. And the other areas of the registry platform are tested before presented in the output which has valuable data. Since the computer world is being extremely huge and complicated and hard drives are getting massively large the investigation job will also need to be more clear to users and investigators, so On registry part too they need to have guide for seeking the data from other point of view.

Therefore some potentially areas could be useful for study and covered on security and investigation aspects:

- Proposing a standard or design for Windows XP or Vista registry platforms which have the ability to limit the alteration, deleting or hiding the data into the keys and have a secure environment.
- Implementation of security with XML based files on Windows Registry files to prevent the corruption of every file when a registry key becoming corrupted.
- Having a security survey on intrusion detection for registry and its authentication approaches to make registry environment more secure.
- Since the lack of having time for every keys and values in windows registry development of an investigation tool for determining the last changed time for all keys and their value is a potential idea.

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*.

APPENDX A

Registry Keys and their Correspondent information

Table A.1: Registry keys and their Forensic Value

Key	Information
HKLM\SYSTEM\CurrentcontrolSet\Hardware Profiles\XXXX	Current Hardware Profile Configurations
HKEY_LOCAL_MACHINE	per Computer Setting
HKCU\Printers\Settings\Wizard\ConnrctMRU\DevModperuser	Most Recently Used Network Printers
HKLM\SYSTEM\MountedDevices	List of Mounted Devices
HKCU\Software\Microsoft\Windows\Current Version\Explorer\MountPoints2\CPC\Volume\	More Information on the Device
HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR	Addition Information about List of Mounted USB Storage Devices
HKLM\SOFTWARE	Software Setting for the Local Machine

HKCU\SOFTWARE	Software Setting that is Users Specific
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App paths HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\currentVersion\Uninstall	Installed Applications Path and Execution Address List
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\currentVersion\Uninstall HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\	Uninstalled Program List SID User Profile List
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWSNT\CurrentVersion\SystemRestore	Stored Restore Points
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32 key	Disabled MRU Files in Registry
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	Order of Listing MRU Files
HKCU\Software\Microsoft\Search Assistant\ACMr	Recent Search Terms
HKCU\Software\Microsoft\Protected Storage System Provider	Windows Protected Storage
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Int	IP Address Interfaces

erfaces	
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	Last Logged On Users
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	Disabled Default Administrator Shares
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	Enable Custom Logon Message
HKEY_CURRENT_USER\Software\Microsoft\MS Setup (ACME)\User Info	Changed Default Name and Company Information
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	Proxy Server Configuration Values
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID	System IP Address and Default Gateway
HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\GUID	Wireless Network Information
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MapNetwork Drive MRU. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2	Mapped Network Drive, Server Name and Shared Folder
HKEY_CURRENT_USER	User Basis Stored Data for Application Key
HKEY_USER\S-1-5-18	Local System Account Identity

HKEY_USER\S-1-5-19	Local Service Account Identity
HKEY_USER\S-1-5-20	Network Service Account
HKEY_USER\S-1-5-21	First Logon on Computer
HKEY_CURRENT_USER\ENVIRONMENT HKEY_CURRENT_USER\IDENTITIES	Microsoft Outlook Express Identity
HKEY_CURRENT_USER\NETWORK	Mapped Drive Windows During User System Logon
HKEY_CURRENT_USER\ SOFTWARE	User-Specific Application Settings
HKEY_CURRENT_USER\VOLATILE ENVIRONMENT	Environmental Variables
HKCU\Software\Microsoft\Windows\Current version\Explorer\ComDlg32	Last Visited MRU Lists Program
HKCU\Software\Microsoft\Windows\Current version\Explorer\ComDlg32\OpenSaveMRU	Most Recent File Opened and Saved
HKCU\Software\Microsoft\Windows\searchA ssistant\ACMrU	Files or Words Search Phrases
HKLM\SOFTWARE\Microsoft\WindowsNT\ CurrentVersion\ Winlogon	User Name of Last Log On
HKEY_LOCAL_MACHINE\SYSTEM\CUR RENTCONTROLSET\CONTROL\TERMIN AL SERVER	Permitted Terminal Services Connections

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation	Systems Time Zone Information
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU	Most Recently Used Files
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	List of Recently Executed Files
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	Executed Files Using the Start>Run Commands
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	Uninstalled Program
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce	Automatically Programs Running Path
HKLM\SYSTEM\CurrentControlSet\Services	Windows Services List
HKCR\exefile\shell\open\command HKEY_CLASSES_ROOT\batfile\shell\open\command HKEY_CLASSES_ROOT\comfile\shell\open\command	Instruction to Execute .exe Extension Files

HKCR\Drive\shell\ and HKCR\Folder\shell\ HKEY_CLASSES_ROOT\batfile\shell\open\command HKEY_CLASSES_ROOT\comfile\shell\open\command	File Execution under Right Click Command in Windows
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist	System Objects and GUID Subkeys
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]	The Source Cause Restricted Access to the Contents of Selected Drives
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]	Specific Applications Restricted From Running
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer].	Disabled Run Command from Registry
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]	Restricted Access to Windows Updated
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]	the Reason Why Registry Editing Tools are Disabled
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]	Hidden Drives in My Computer

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]	Disables Shutdown Command
[HKEY_CLASSES_ROOT\CLSID\{5b4dae26-b807-11d0-9815-00c04fd91972}]	Disable Menu Bars and the Start Button
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]	Hidden Control Panel, Printer and Network Settings
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]	Disabled User Tracking
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\ TypedURLs]	Cleared Internet Explorer Typed Address History from Registry