FORENSIC ANALYSIS OF WINDOWS REGISTRY AGAINST INTRUSION

Haoyang Xie[1], Keyu Jiang[1], Xiaohong Yuan[2] and Hongbiao Zeng[3]

[1]Department of Informatics, Fort Hays State University, Hays, KS, US
kjiang@fhsu.edu
[2]Computer Science Department, North Carolina A&T State University, Greensboro, NC, US
xhyuan@ncat.edu
[3]Department of Math and Computer Science, Fort Hays State University, Hays, KS, US
hzeng@fhsu.edu

ABSTRACT

Windows Registry forensics is an important branch of computer and network forensics. Windows Registry is often considered as the heart of Windows Operating Systems because it contains all of the configuration setting of specific users, groups, hardware, software, and networks. Therefore, Windows Registry can be viewed as a gold mine of forensic evidences which could be used in courts. This paper introduces the basics of Windows Registry, describes its structure and its keys and subkeys that have forensic values. This paper also discusses how the Windows Registry forensic keys can be applied in intrusion detection.

KEYWORDS

Forensics, Information Security, Windows Registry

1. INTRODUCTION

In a digital age, information has become an important resource that people depend on in every aspect of their lives. With the development of computers and networks, the communication of information becomes faster and faster. Fast internet access makes it possible to create social networks and share news and events across the world quickly. However, as people enjoy the convenience of information access and transfer, the risks of security and privacy problems increase greatly too. People with malicious motives use sophisticated technology as a tool to access information they are not authorized to access. With these malicious actions computer and network forensics emerged as a discipline. Computer and network forensics is the abbreviation of computer and network forensic science. It includes a number of fields such as hard drive forensics, remote forensics, mounted devices forensics, Registry forensics, and so on. In this paper we focus on Windows Registry forensics which is an important branch of computer and network forensics.

By the time this research was conducted, Windows XP had been accepted widely and was the most stable Windows desktop operating system (OS). Therefore, Windows XP was used as the basic operating system in this research. The Registry structures of Windows XP and Windows 7 are very similar and both of them have the same root keys.

Microsoft has warned its customers to keep away from the Registry --Windows's heart -- since it stores all of the computer settings and is very complex. Windows Registry contains all of the

DOI : 10.5121/ijnsa.2012.4209

configuration settings of specific users, groups, hardware, software, and networks. However, hackers often explore and alter the keys and values in Windows Registry to attack a computer or leave a backdoor. However, the operations that hackers performed could be found by investigators as evidences. This paper introduces the basics of Windows Registry, and discusses how the Windows Registry keys and subkeys can be applied in intrusion detection.

This paper is organized as follows: Section 2 introduces the Windows Registry basics and the structure of Windows Registry. Section 3 examines forensic keys in Windows Registry. Section 4 discusses how to apply forensic keys in intrusion detection.

2. The Windows Registry Basics

Windows Registry is a central repository or hierarchical database of configuration data for the operating system and most of its programs [1]. It contains abundant information that has potential evidential value in forensic analysis [11]. Windows Registry Editor can be used to access Windows Registry. Windows Registry Editor can be started by using the "run" command to run the "regedit.exe" file. Figure 1 shows the Windows Registry Editor when it is started.

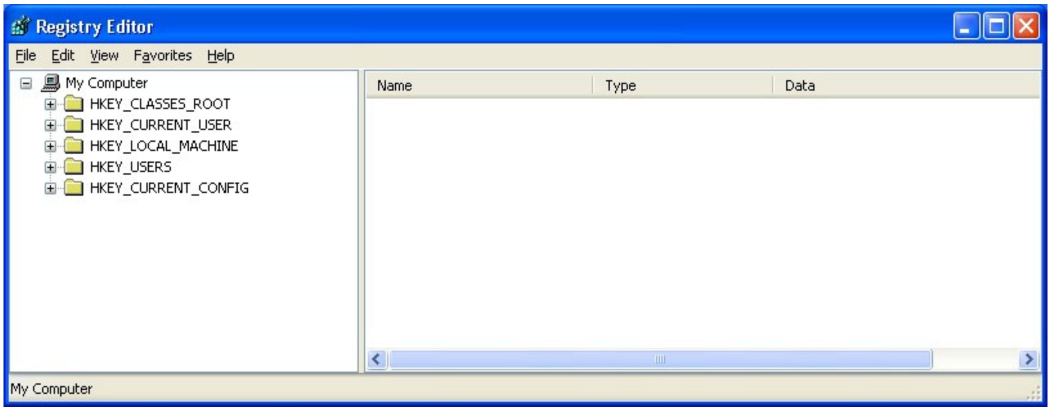


Figure 1. Windows Registry Editor

2.1. The History of Windows Registry

The root of Microsoft operating system was MS-DOS, which was a command line operating system. In the DOS age, there was no registry but two files designed to store the configuration information: "config.sys" and "autoexec.bat". "Config.sys" was used to load the device drivers and "autoexec.bat" was used to store the configurations of running programs and other environmental variables [8]. When the first graphical interface operating system of Microsoft, Windows 3.0, was released, these two files used in MS-DOS were replaced by INI files. These files were used to store the configuration settings of the computers.

In Windows 95, a hierarchical database named Registry was introduced [6]. Although the Registry of Windows 95/98 has the similar structure as Windows XP/Vista/7, the amount of data in Windows XP/Vista/7 Registry has grown tremendously. The Registry in Windows XP/Vista/7 has a more stable and complex structure than Windows 98/95/2000. In addition, the structure of Windows XP registry could be considered as the basis of modern Windows

Registry. Although Windows Vista/7 Registry has more content than Windows XP registry, it has very similar structures, keys, subkeys, and values as Windows XP registry.

2.2. The Structure of Windows Registry

The Windows Registry Editor is divided into two panels (Figure 1), the left one is key panel and the right one is value panel. In the left panel, there are five root keys, HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, and HKEY_CURRENT_CONFIG. These root keys form the basic structure of Window Registry. However, this structure is just a logical structure [9]. Among these five root keys, only two root keys, HKEY_LOCAL_MACHINE and HKEY_USERS, have physical files or hives. These two keys are called master keys. The other three keys are derived keys since they are derived from the two master keys and their subkeys, or, they only offer symbolic links to the two master keys and their subkeys [1].The five root keys and their subkeys are described below.

(1) HKEY_LOCAL_MACHINE (abbr. HKLM). HKLM is the first master key. It contains all of the configuration settings of a computer. When a computer startups, the local machine settings will boot before the individual user settings. If we double-click this entry in Windows Registry Editor, five subkeys will be listed: HARDWARE, SAM, SECURITY, SOFTWARE, and SYSTEM. The information contained by these subkeys are listed below:

- HARDWARE is used to store the information of hardware devices that a computer detects when the computer starts up. So, the subkeys in HARDWARE are also created during the booting process.
- SAM is the abbreviation of Security Account Manager which is a local security database. Subkeys in SAM contain the setting data of users and work groups.
- SECURITY includes a local security database in SAM and a strict ACL is used to manage the users who could access the database [8].
- SOFTWARE includes all of the configuration settings of programs. Information on the programs is stored in a standard format: HKLM\Software\Vendor\Program\Version.
- SYSTEM contains the configuration settings of hardware drivers and services. The key path is HKEY_LOCAL_MACHINE\SYSTEM\ControlSetXXX, where XXX is a three digital number from 000, as shown in Figure 2.

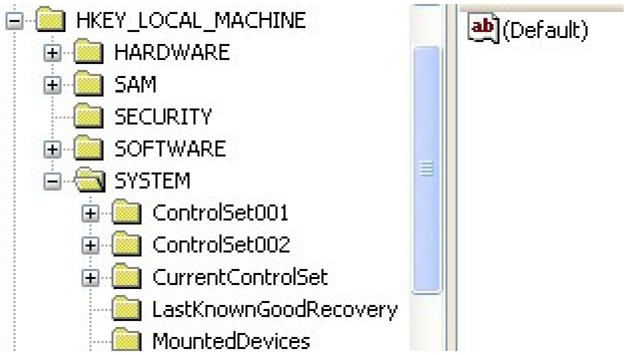


Figure 2. HKEY_LOCAL_MACHINE Root Key and Its Subkeys

(2) HKEY_USERS (abbr. HKU). HKU is another master key. It contains all of the per-user settings such as current console user and other users who logged on this computer before. Double-click this entry, we can see at least three kinds of subkeys listed: KEFAUTL, SID, and SID_CLASS [1]. SID is security identifier which refers to the current console. SID-CLASSES contains per user class registration and file association. Usually, we could see S-1-5-18, S-1-5-19, and S-1-5-20, which represents Local System Account, Local Service Account, and Network Service Account respectively [3].

Unlike the above two keys, HKEY_CLASSES_ROOT (abbr. HKCR), HKEY_CURRENT_USER (abbr. HKCU), and HKEY_CURRENT_CONFIG (abbr. HKCC) are derived keys and they only link to the two master keys and their subkeys.

(3) HKEY_CLASSES_ROOT (abbr. HKCR). HKCR contains two keys: HKLM\SOFTWARE\Classes and HKCU\Software\Classes. The first one refers to the default registration classes, and the second one refers to per user registration classes and file associations.

(4) HKEY_CURRENT_USER (abbr. HKCU). HKCU links to a subkey of HKU, HKU\SID. This key allows all of the Windows programs and applications to create, access, modify, and store the information of current console user without determining which user is logging in [10].

Under the root key HKCU, there are also five subkeys: Environment, Identities, Network, Software, and Volatile Environment.

- Environment is about the environmental configurations.
- Identities are related to Outlook Express.
- Network contains settings to connect the mapped network drive.
- Software refers to the user application settings.
- Volatile Environment is used to define the environmental variables according to different users who logon a computer.

(5) HKEY_CURRENT_CONFIG (abbr. HKCC). HKCC is an image of the hardware configuration profiles. HKLM\SYSTEM\Current\ControlSet\Hardware\Current, is also a link to HKLM\SYSTEM\ControlSet\Hardware Profiels\XXXX, where XXXX is a four digital number from 0000.

2.3. Values

If we compare the Windows folders and files with Windows Registry, then the keys and subkeys could be considered as folders and sub folders, and the values of a key could be considered as the files in a folder. Just like a file of Windows, a value also has its properties. Name, type, and data are the three components of a value. Every value has a unique name. The naming regulations are also similar to those of files. Some special characters such as “?”, “\”, and so on could not appear in the name of a value [5]. There are six major types of values: string, multistring, expandable string, binary, Dword, and Qword.

- String values are the easiest to understand because data in this type is recorded in plain text in English.

- Multistring values include a list of strings with ASCII code 00 separating these strings [4].

- Expandable string is another variant of string value. Expandable string contains special variables such as %SYSTEMROOT%, %USERPROFILE% and so on. These variables could replace some special path easily. For example, if we want to locate the folder X:\Documents and Settings\username\Desktop, the %USERPROFIEL%\Desktop could be used no matter on which drive windows are installed and which user logs on.

- Binary value also stores string but the data is displayed in hex format and the information stored is always related to hardware [7].

- Unlike the above value types, the data stored in Dword and Qword are not strings of characters. There are two numbers in Dword and Qword types: 1 and 0 (usually 1 for enable and 0 for disable). In some cases, numbers within 60 are used to indicate data related to timeout settings. However, the difference between Dword and Qword is that Dword stores 32-bit data and Qword stores 64-bit data [6].

2.4. Hives

Hives are the physical files of the two master keys in Windows Registry stored on hard drive. The tree format we view through Windows Registry Editor, as shown in Figure 1, is a logical structure of the five root keys. If we use forensic tools to view the Windows Registry in an offline environment or view the Registry remotely, only the two master keys will be listed. So only the two master keys and their subkeys have hives. The hives of HKLM's subkeys are stored at %SYSTEMROOT%System32\config, and the hives of HKU's subkeys are stored at %USERPFOFILE%.

3. RELATED WORK

Derrick J. Farmer explores the Windows registry by examine the MRU List, UserAssist, Wireless Networks, USB devices, Internet Explorer, Windows passwords, instance message applications and etc. [3] Lih Wern Won discussed the data hided in Windows registry in his research and illustrate some techniques to hide data into the registry and registry keys.[4] Both researchers agree that Windows registry is a very important source for forensics evidence and understanding the type of data could reside in the registry is crucial in the forensic analysis process.[3][4]

4. FINDINGS ON FORENSIC KEYS

Because the five root keys have different functions, the subkeys under them have different functions as well. During this research, every subkey of the five root keys was checked. The keys and subkeys that have forensic value were filtered and organized into three sections: software, hardware, and network, as shown in Table 1. Windows Registry Editor is the main tool used to view the Registry. AccessData's Registry Viewer (Demo version) [2] was also used during the research process. However, because of the limitations of the demo version, lots of functions are disabled.

Table 1 lists the keys filtered from every subkey that has forensic value under the five root keys. We discuss some applications of the keys that have forensic value in the next section.

Table I. Keys with Forensic value

Key	Description
Software	
HKEY_LOCAL_MACHINE|SOFTWARE\Microsoft\Windows\CurrentVersion\Program Path	Install Apps
HKEY_LOCAL_MACHINE|SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	Uninstall Apps
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList	SID Profiles
HKLM\SOFTWARE\MICROSOFT\WindowsNT\CurrentVersion\System Restore	Restore Points
HKLM\SOFTWARE\Classes	Class Registration and Files Association
HKCU\Software\Classes	Per-user settings
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32	Most Currently Used Files
KHCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	MRU order
HKCU\SOFTWARE\Microsoft\Search Assistant\ACMru	Recently Search
HKLM\Software\Microsoft\Command Processor	AutoRun
KHCU\Software\Microsoft\Protected Storage System Provider	Windows Protected Storage
HKLM\System\CurrentControlSet\Services\Tcpiip\Parameters\interfaces	IP
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	Last Logon Users
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32	Last Visited MRU
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU	Open and Save of Recent Files
HKCU\Software\Microsoft\Windows\SearchAssistant\ACMru	Files and words searched
Hardware	
HKLM\SYSTEM\CurrentControlSet\HardwareProfile\XXXX	Current Hardware Settings
HKLM\SYSTEM\MountedDevices	Mounted devices
HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR	USB Devices

Network	
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID	IP Address and Gateway
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MapNetworkDriveMRU	Mapped Network Devices

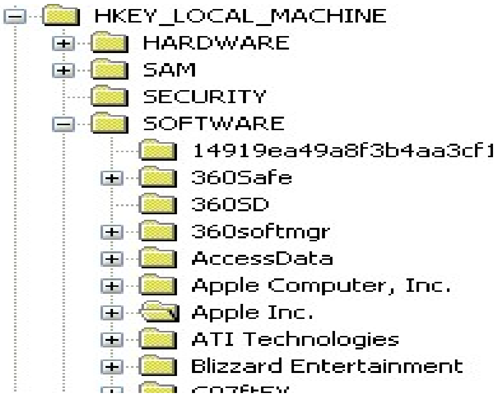
5. DISCUSSIONS ON THE APPLICATIONS OF THE FORENSIC KEYS

In the previous section the keys that could be used to conduct forensic analysis are filtered and organized. This section demonstrates how to use these keys and related software to find reliable evidence in the investigation of an intrusion case. Several applications of these forensic-valuable keys are introduced. These applications are related to software subkey, firewall and security center of Windows, security identifiers, and user activities.

5.1. Forensic Evidence in Software Subkey

Software subkey could be easily found from different root keys. However, only the two master keys have hives. So here we discuss HKLM\SOFTARE which is located in the hives called software, with physical address %SYSTEMROOT%\System32\Config\software. This software subkey contains software configuration settings for the local computer. Other software subkeys such as HKEY_Current_User\software stores user specific settings about the software installed in a computer.

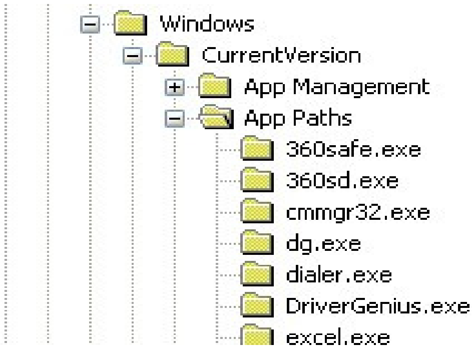
Software subkey includes information about software including logon information. When a program is installed on a computer, the registry records the installation at the same time. Even if a program has been uninstalled from a computer, the information about the program could still be found in Windows Registry but the location may be different. In intrusion incidents, most of the compromised computers are installed some kind of malicious software like virus or Trojan horse. Although the process of installation is hidden by hackers, information about the malicious codes could be found in Windows Registry. In this case, the exact locations of these malicious codes could be found. The first place that should be checked is the root of software subkey as shown in Figure 3. A list of software or company names is shown under software subkey.



```
HKEY_LOCAL_MACHINE
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
        14919ea49a8f3b4aa3cf1
        360Safe
        360SD
        360softmgr
        AccessData
        Apple Computer, Inc.
        Apple Inc.
        ATI Technologies
        Blizzard Entertainment
```

Figure 3. The root of software subkey

Besides the root of software subkey, there are still two more locations that could be checked if the information we want is not under HKLM\SOFTWARE. One such location is: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Path. Programs with executable names are listed at this location, for example, every name listed in Figure 4 has an extension .EXE.



Windows
CurrentVersion
App Management
App Paths
360safe.exe
360sd.exe
cmmgr32.exe
dg.exe
dialer.exe
DriverGenius.exe
excel.exe

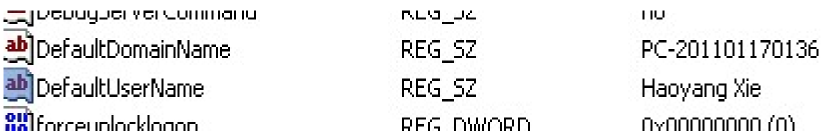
Figure 4. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Path

HKLM\SOFTWAR\Microsoft\Windows\CurrentVersion\Uninstall is another location that should be checked. The location includes information about the software that has been removed.

Usually, it's quite easy to find the information we want in one of the above locations. In a network intrusion case, investigators almost always need to determine which software has been installed in a computer. If special forensic tools are not available, the investigators have to look from many locations for the software to locate its physical path.

Time and date information are also important in some cases. Hackers often change the created, accessed, and modified times of their malicious programs in order to make the victims think that these software have been in their computers for a while. However, the last written time in Windows Registry is often true. The hackers often overlook this timestamp because Windows Registry Editor does not include the timestamp. If we could find the last written time, then we can determine the time the hacker attacked the computers. The timestamps could also narrow the range of the logs we should check. Although timestamp couldn't be viewed by Windows Registry Editor, it can be viewed with the help of other tools such as AccessData's Registry Viewer (Demo version).

Under HKLM\SOFTWARE, the last logon user could also be found and the exact key path is HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon. This key contains the last logon information, as shown in Figure 5. The value named DefaultUserName corresponds to the information about the last logon user. In Figure 5, Haoyang Xie is the last logon user. DefaultDomainName is PC-201101170136. The string of numbers is actually the time when the Windows OS was installed on a computer, by default setting.



```
DebugServerCommand        REG_SZ        no
DefaultDomainName         REG_SZ        PC-201101170136
DefaultUserName           REG_SZ        Haoyang Xie
forceunlocklogon          REG_DWORD     0x00000000 (0)
```

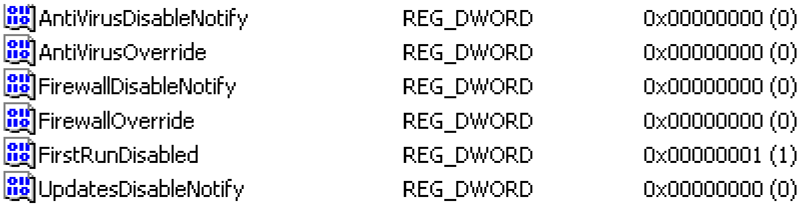
Figure 5. Information on the last Logon User

5.2. Forensic Keys Related to Firewall and Security Center

Windows firewall came with Windows XP SP2. It lacks features that most software firewalls have. This firewall could be considered as a significant improvement on Windows security. In addition to the firewall, Windows also offer a security center which is used to notify the situations of Windows update, firewall, and antivirus. If one of them is disabled, the security center will notify the users right away.

Hackers would hope that all of the computers in the world lack basic protection so that they could hack into the computers easily. In the real world, most of the computers have certain protection. Hackers want to overcome the obstacles in order to manifest their sophisticated hacking skills. During the hacking process, attackers try to invade other users' computers without causing any warnings for the users. So when they try to intrude a Windows-based system, the notification of Windows security center would be the first obstacle to overcome. For most of intruders, the "standard process" is to disable all of the notifications first, then turn off the firewall and the antivirus software. After that they could invade the computers any way they want based on their skills.

For Windows security center, all of the settings could be changed in its graphical interface. However, it's more convenient for an intruder to change the settings in Windows Registry to disable the notifications of Windows security center. The configurations about Windows security center are stored in HKLM\SOFTWARE\Microsoft\Security Center, as shown in Figure 6.



```
AntiVirusDisableNotify    REG_DWORD     0x00000000 (0)
AntiVirusOverride         REG_DWORD     0x00000000 (0)
FirewallDisableNotify     REG_DWORD     0x00000000 (0)
FirewallOverride          REG_DWORD     0x00000000 (0)
FirstRunDisabled          REG_DWORD     0x00000001 (1)
UpdatesDisableNotify      REG_DWORD     0x00000000 (0)
```

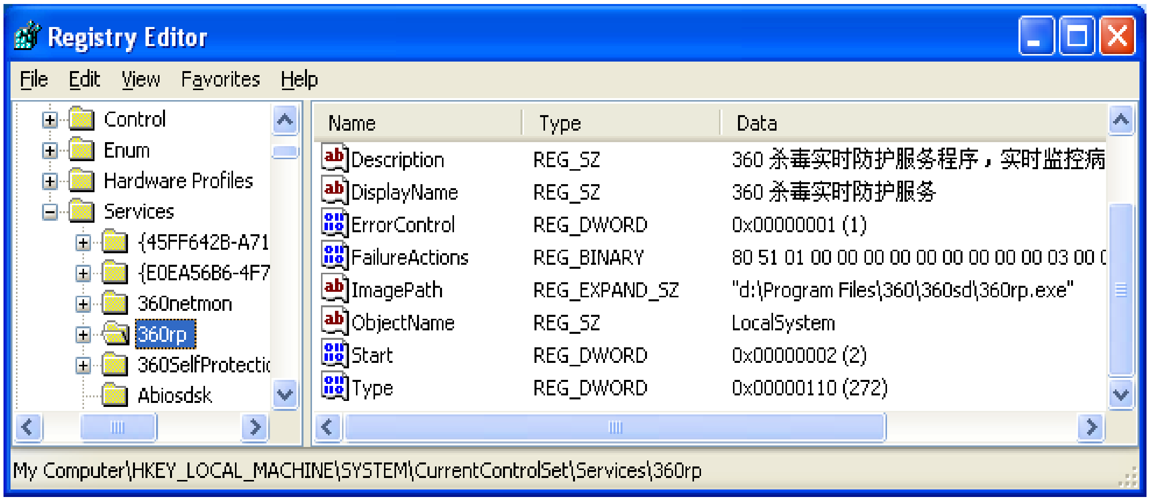
Figure 6. Configurations about Windows security center in Windows Registry

As shown in Figure 6, the functions of the values could be identified by their names easily. If the data of the "notify" value is 0, the notification is enabled, otherwise it is disabled.

In addition to the notification information about security center, the configurations of firewall are stored in HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy. This key includes two subkeys: StandardProfile and DomainProfile. StandardProfile is the local profile and the DomainProfile is per group's settings. Both of them could be controlled by a

DWORD type value EnableFirewall. If the data is 1, then the firewall is enabled, and the firewall works normally. If the data is 0, the firewall is disabled. Sometimes, we couldn't find the EnableFirewall value under these two profile keys. Then we may create a new value named "EnableFirewall" with DWORD type. In addition, a subkey named AuthorizedApplications is listed under each Profile. Some intruders could also use .reg file to allow their malicious codes to access the compromised systems. In this situation, an intruder doesn't even need to disable the notifications.

The last step is to disable antivirus. Often antivirus boots with the startup of a computer. We have known that the key path of services is HKLM\SYSTEM\CurrentControlSet\Services, as shown in Figure 7. Each subkey of the Services key has a DWORD value named "Start" which indicates the ways of booting. If the data is 2, this service will start up with the boot of Windows. If the data is 3, the service will be started manually. If the data is 4, the service is disabled. In Figure 7, the highlighted subkey 360rp is related to the antivirus software and the "Start" data is 2. If a hacker wants to bypass the security control of the desktop, he will set the "Start" data to 4 to disable 360 Safety to avoid the antivirus software.



Name	Type	Data
Description	REG_SZ	360 杀毒实时防护服务程序，实时监控病
DisplayName	REG_SZ	360 杀毒实时防护服务
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	80 51 01 00 00 00 00 00 00 00 00 00 03 00 (
ImagePath	REG_EXPAND_SZ	"d:\Program Files\360\360sd\360rp.exe"
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000110 (272)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\360rp

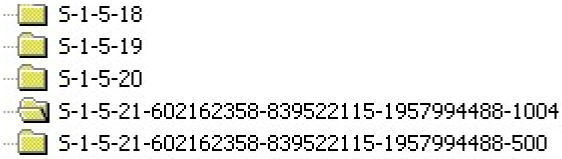
Figure 7. The key path of services

Investigators have to be familiar with the processes hackers use so that they could check the correct locations as soon as possible when an intrusion occurs. Timestamp is also very important. For network intrusion, intrusion time is very important to forensics.

5.3. Forensic Evidence from Security Identifiers

Each user, group, and computer is assigned a Security Identifier (SID). Access Control List also uses SIDs to distinguish different users and groups. In most real cases, it's impossible to know the usernames or group names in a computer. SIDs are the only identifiers for different users and groups. In addition, the locations of SIDs are very easy to find.

Under HKU, we could find the SIDs as shown in Figure 8. Usually the long strings stand for different users.

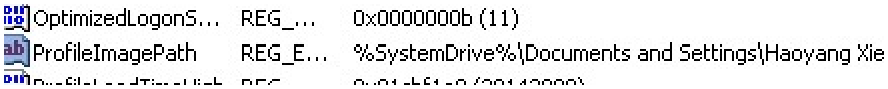


```
S-1-5-18
S-1-5-19
S-1-5-20
S-1-5-21-602162358-839522115-1957994488-1004
S-1-5-21-602162358-839522115-1957994488-500
```

Figure 8. SIDs inWindows Registry

Figure 8 shows there are two users in this computer. The longest string is S-1-5-21-602162358-839522115-1957994488-1004. "S" indicates that the following string is a SID. The first number "1" is the revision number. The third part is the authorized level which ranges from 0 to 5. The fourth part is the local or domain machine identifier. In this example, 602162358-839522115-1957994488 is the local computer identifier. The last part "1004" is a relative identifier which is also a unique number within a local computer or domain [2].

However, what we see here is just a set of numbers. If there are large amount of strings of numbers, and we are not familiar with the settings of a computer, then we could not know which user a SID stands for. In Registry Forensics, it is necessary to map SIDs to users. The mapping between SIDs and users is stored in SAM, a local security database. With the help of specific forensic tools, this problem could be resolved easily. If forensic tools are not available, there is also a manual method that could be used to identify the users. In a Windows system, the username could appear in "My Documents". If we could find the relationship between SIDs and "My documents", we may resolve the mapping of SIDs to users.



```
OptimizedLogonS...   REG_...   0x0000000b (11)
ProfileImagePath     REG_E...  %SystemDrive%\Documents and Settings\Haoyang Xie
```

Figure 9. Profile Image Path in Registry

Fortunately, This is possible. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList offers a set of subkeys like HKU. The SID S-1-5-21-602162358-839522115-1957994488-1004 could also be found here. Locate S-1-5-21-602162358-839522115-1957994488-1004 and check its value. A value named ProfileImagePath as shown in Figure 9 indicates the path of "My documents" and the username of the SID is "Hoayang Xie". The other SID ended with 500 is the default username "administrator". In Figure 8, we find that the two SIDs are identical except for the last section which means the two users are in the same domain. Therefore SIDs can also be used to define which domain a user belongs to.

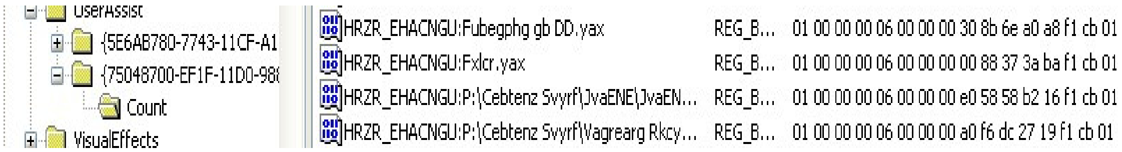
As a unique identifier, SID is very important. In real cases, investigators always use SIDs to look for the targets they want to focus on. If they use professional forensics tools, they could resolve every part of the SID, which may provide more useful information for forensics.

5.4. Forensics Evidence about System Access through User Activities

User activities include all of the actions that users have performed on a computer. Here we only focus on those actions that may provide useful information for investigation. In Windows Registry, most of the user activities are recorded in "ntuser.dat". Just as the software hive stores all of the configuration settings of local machine, the “ntuser.dat” stores all of the settings for specific users. HKCU\Software subkey contains information about the installed software, and the major activities that the users performed on the software. In addition, this software subkey also includes specific user data such as searches, command, username, password, and so on.

The first location we need to discuss is Most Currently Used (MRU) which is used to store commands and usernames that users entered. For example, the “run” command always displays a drop down list which lists the recent commands that was entered into the “run” dialogue. In Windows Registry, we could also find many keys with a suffix MRU. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU stores the information in the “run” command drop down list. According to the order of the values in the value panel, we could know which command is the most recent one. Advanced hackers always use “run” command rather than graphical interface. When an investigator investigates an intruder’s computer, according to the commands the intruder entered and the timestamps, the investigator may be able to decide what the intruder did and when. Besides the “run” commands, other actions could also be recorded such as the URL typed in Internet Explorer, the opened DOC files, and so on. Rich information about MRU is stored in different subkeys and they could offer important clues in a real case.

Another important location an investigator has to check is UserAssist key which includes significant information about users’ activities. The key path of UserAssist is HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count, as shown in Figure 10. This subkey contains a list of values with odd names. Actually, the value names are encoded by ROT 13 which means that the character is rotated 13 characters. With professional forensic tools, the names could be decoded easily.

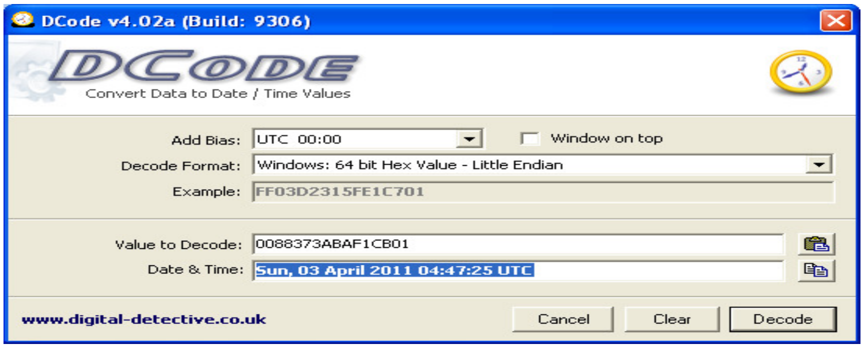


```
UserAssist
  {5E6AB780-7743-11CF-A1
  {75048700-EF1F-11D0-98
    Count
VisualEffects
```

```
HRZR_EHACNGU:Fubegphg gb DD.yax                REG_B...   01 00 00 00 06 00 00 00 30 8b 6e a0 a8 f1 cb 01
HRZR_EHACNGU:Fxlcr.yax                         REG_B...   01 00 00 00 06 00 00 00 00 88 37 3a ba f1 cb 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\JvaENE\JvaEN...  REG_B...   01 00 00 00 06 00 00 00 e0 58 58 b2 16 f1 cb 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\Vagrearg Rkcy... REG_B...   01 00 00 00 06 00 00 00 a0 f6 dc 27 19 f1 cb 01
```

Figure 10. The key path of UserAssist

The data of the values can offer very useful evidences. The data is 16-byte. The first 4-byte is for unknown information at this time; the next 4-byte is a counter designed to record the times a program has been run [2]. The last 8-byte is a Windows 64-bit timestamp which indicates the last time a program was run. The counter, the middle 4-byte, starts with number 6 when a program runs for the first time. Compared with the counter, the timestamp indicated by the last 8 bytes is more important. Some professional tools, such as AccessData’s Registry View (Full License) [12] and EnCase [13], could decode all of the data including the timestamps, counters, and value names. If these tools are unavailable, we could use another free tool Dcode (Demo) [14] to decode the data. For example, the second value’s last 8-byte data is 88 37 3a ba f1 cb 01, which is decoded to “Sun, 03 April 2011 04:47:25 UTC”, as shown in Figure 11.


DCode v4.02a (Build: 9306)
DCODE
Convert Data to Date / Time Values
www.digital-detective.co.uk
Cancel
Clear
Decode

Add Bias: UTC 00:00

□ Window on top

Decode Format: Windows: 64 bit Hex Value - Little Endian

Example: FF03D2315FE1C701

Value to Decode: 0088373ABAF1CB01

Date & Time: Sun, 03 April 2011 04:47:25 UTC

Figure 11. Decode the data of the values using Dcode

Besides these, there is still more information about user activities such as the information about Protected Storage System Provider, which stores some usernames and passwords. However, without professional forensic software, we could not read the information. In addition, there is still more information about MRU which could be found at different locations for different programs.

6. Conclusion

Windows Registry Forensics is a very important branch of computer and network forensics. The real cases are more complex and different forensic tools need to be used together to achieve enough evidence. This paper focuses on Windows Registry Forensics. Keys and subkeys that have forensic value are filtered from Windows Registry and organized. They could be considered as tools to investigate Windows Registry in real cases. As part of Windows Registry forensics, this paper discusses the applications of the forensic keys against intrusion. However, the keys filtered and organized in this paper are not all of the keys that have forensic values. Windows Registry is huge and the research on it continues. Even if we have known every key, subkey, and value of Windows Registry, we still have to consider how to use them in real cases since the intrusion cases will not be the same every time.

References

[1] Anson, S., & Bunting, S. (2007). Mastering Windows Network Forensics and Investigation. Indianapolis: Sybex.

[2] Carvey, H. (2011). Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry. Burlington: Syngress.

[3] Farmer, D. J. (n.d.). A forensic analysis of the Windows Registry. Retrieved March 13, 2011, from http://www.forensicfocus.com/downloads/windows-registry-quick-reference.pdf

[4] Ferri, V. (n.d.). Registry Data Types. Retrieved March 13, 2011, from http://pubs.logicalexpressions.com/pub0009/LPMArticle.asp?ID=361

[5] Fisher, T. (n.d.). Registry Value. Retrieved March 10, 2011, from About.com PC Support: http://pcsupport.about.com/od/termsv/g/registryvalue.htm

[6] Honeycutt, J. (2005). Microsoft Windows Registry Guide. Redmond: Microsoft Press.

[7] Ivens, K. (2001, March 19). Registry Data Types. Retrieved March 14, 2011, from http://www.windowsitpro.com/article/registry2/registry-data-types.aspx

[8] Kamara, L. (n.d.). The Windows Registry Overview. Retrieved March 11, 2011, from http://ezinearticles.com/?The-Windows-Registry-Overview&id=2274356

[9] Microsoft Corp. (n.d.). Registry Editor overview. Retrieved March 11, 2011, from http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/regedit_overview.mspx?mfr=true

[10] Microsoft. (2008, February 4). Microsoft Support. Retrieved March 11, 2011, from Windows registry information for advanced users: http://support.microsoft.com/kb/256986

[11] Wong, L. W. (n.d.). Forensic Analysis of the Windows Registry. Retrieved March 15, 2011, from http://www.forensicfocus.com/downloads/forensic-analysis-windows-registry.pdf134

[12] AccessData, Registry Viewer. Retrieved February 17, 2012, from http://accessdata.com/support/adownloads

[13] Guidance Software, EnCase Forensic, Retrieved February 20, 2012, from http://www.guidancesoftware.com/forensic.htm

[14] Digital Detective, Free Tool-DCode. Retrieved February 20, 2012, from http://www.digital-detective.co.uk/freetools/decode.asp