Ali *et al.LGU (IJECI)* 2018

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 3 July-September 2018

Role of Windows Registry Forensics in Digital Forensics Investigation

Mohsin Ali[1]
Digital Forensics Research and Service Centre
Lahore Garrison University, Lahore, Pakistan
mohsinaly@lgu.edu.pk

Abstract:

The research paper covers one of the most important aspect of the digital forensics investigation "Registry Forensics" as there are several components that are necessary for carrying out digital forensics investigation, one cannot overall the windows registry. The research paper is basically divided into two segments, where the first segment fully explains what registry is, how it works, and what important information stored in it. Moreover, the research paper covers the aspect of anti-forensics elements that are incorporated by different cyber criminals in order to wipe the traces of fraudulent activities, and finally the author has concluded the research paper by highlighting the importance of windows registry in digital forensics investigation.

Keyword: Digital Forensics, Forensics Investigation, Windows Registry, Windows Registry Forensics, cybercrime, cybercriminal.

1. Introduction

As there are many aspects that are examined by an investigator during the investigation of a criminal offence same goes with the digital forensics investigation, after seizing the crime scene the investigating officer has to take forensics image of the suspect system, after that it is taken to the forensics labs for the examination, the investigator here critically analyse every aspect of the image, and look for the foot prints that can help him in drawing his findings. One of the most important element that is analysed during the examination phase of the investigation is the examination of windows registry. To start with windows registry is the fundamental component of windows OS Operating system, which contains a lot of information regarding the configuration of the system. The information that is managed within the registry of the windows contains the history of the user activities, details about the program installed and details about the running programs. The storage of data is carried out in same way as it is done in log file [1]. Windows registry is explained in depth in proceeding parts of this research paper.

2. Literature Review

In order to support the stance of role of windows registry in digital forensics investigation, the author has studied different related work. After studying various literatures, the following keys are highlighted and are explained in depth.

2.1 What Is Windows Registry?

The explanation that is derived from the Microsoft's publication regarding registry, is that it's a database that contains the important information category wise pertaining to the application, services and operations that are running on the windows [2]. The format that is used to structure the data in registry is of tree format. The tree is consists of several nodes, these nodes are known as keys. Then there is further classification of these keys, where each key is consist of subkeys and entries of data known as values. In some cases the only a single key is sufficient for an application to run or to perform the operations, and sometime it is necessary for an application to open a key and to use the values that are linked with that particular key. There is no limits to the amount of values that a key can have, and neither it's mandatory that values should be in one particular form, values can exists in any form [3].

Since windows registry deals with the critical operations of the windows operating system therefore it's certainly not wrong to say that the operations are directly linked to the system, and user of the windows. Windows registry is critical to this extent that every time when an application runs on a windows machine the first thing that's been done by an application is that its record in registry, it's technically not possible for any application to start without accessing the registry. Just to make things further clear, if at any point registry fails the operating system of the windows machine will fail [4].

2.2 Structure of Registry:

The structure of the registry is basically comprised of the repetition of the same pattern of folders called subtrees, keys and subkeys. The lowest level of data that is stored in the registry are the entries. Entries are similar to the files. The repetitive container leads up to the path to each entry, as every individual entry in the registry has a unique path, every entry that is within the registry is referred by its name and complete path. [5]

For accessing the windows registry in normal condition (Not for forensics investigation) we use windows registry editor tool "regedit.exe". The following section of the research paper is about the components that a typical registry contains.

2.2.1 Subtree:

The subtree is classified as the primary or the root segment of the registry. In a registry there are basically 5 core sub trees, that is further divided in keys, subkeys and entries everything that is within these keys and subkeys it has some values. The name of the value and the data of the value can consist of backslash characters or keys. The 5 main subtree are as follow.

1. **HKEY_CLASSES_ROOT**
2. **HKEY_CURRENT_USER**
3. **HKEY_LOCAL_MACHINE**
4. **HKEY_USERS**
5. **HKEY_CURRENT_CONFIG**

Figure 1: The main keys in a windows registry.

2.2.2 Key:

Once a subtree is expanded the first layer that a viewer can witness is of the key, key is the division of the registry that must contain minimum one subkey (like Hardware Key). One thing that is very important here is that some subtrees does not have a key at all.

2.2.3 Subkey:

The when keys are further expanded to one level down one can view the subkeys. Moreover, there can be subkeys that are directly under the expansion of the keys as mentioned earlier that some subtrees do not have any key, so in such cases those subtrees have subkeys. The role of the subkeys is that it is used to save the entries and additional subkeys.

2.2.4 Entry:

Once the expansion of subtree reaches the lower level in the registry, the entries appear, these entries appear in the right-hand side pane of the registry window. Each registry is consists of the name of the entry followed by the its Data types in the registry (the Data type of the registry is used for identifying the format of the data and the length of the data which is to be stored in the entry) and finally a field which is called value. Data is stored within the value field of the registry. Each entry is identified by its name and path. The role of the entries in the registry is to maintain the configuration information of the windows program and windows itself. Entries are entirely different than subtrees, keys and subkeys as they exists in form of folders only whereas the actual information is within the entries.

2.2.5 Hive Files:

The Hive Files are those files which contains the files that are permanently stored in the registry of the system. The location to check these hive files is in the hivelist subkey in HKLM\SYSTEM\CurrentControlSet\Control. These files are updated every time a user login the system the storage location of these registry files is in systemroot\System32\ Config folder. Within HKEY_LOCAL_ MACHINE there are four to five hive files that are stored, and there is one file that is stored within the HKEY_USERS. The Hive files that are within the registry are as follow:

SAM: SAM basically stands for Security Accounts Manager, it possess data which is stored in HKLM\SAM which is related to the service of security of the Accounts management.

SECURITY: As the name suggests it carries the information that is relevant to the security of the system. The information pertaining to this hive is saved in HKLM\Security key.

SOFTWARE: everything which is relevant to

the configuration of system software configuration is saved in HKLM\SOFTWARE keys.

SYSTEM: This hive file has the information regarding the system configuration the data for this hive file is saved in HKLM\SYSTEM key. **DEFAULT**: The purpose of this hive file is to maintain the default system information, all the data related to this hive is saved in HKEY_USERS\.DEFAULT key.

HKEY_LOCAL_MACHINE\HARDWARE this particular hive is not saved as file as it is recreated by the system every time system boots up.

2.3 Variability of the Registry:

It's certainly not possible that two registries are the same, it's because each registry saves the information about the hardware and the software which exists on the system or is installed, the values that are within the registry entries are precisely according to the system and it's configuration. There are few entries that are only created when the windows machine is turned on or the time when the user log on.

As mentioned before that each entry has a specific location, that location can be changed, sometime it happens when a program is updated. There are few registry which shifts the whole program to new location when a minor change is made to the program such as enabling of one particular service.

Since there is variation in the location of registry it is not advisable for a programmer or script writer to write a script that directly refers to any entry in the registry, this can cause problem in the operations of the program if specifically not pointed to the required registry entry, there is another possibility with registry is that with the change in the version of the registry the program written to fetch specific registry entry might change, for all such purposes the recommended application programming interference (APIs) is win32 API, it's because win32 API is updated each time version is changed.

2.4 How Registry Data is Used:

One of the most important and critical reason to study about registry is how data is stored in Registry or the mechanism of storing data into the registry. There are several types of data that are stored by a program in the registry. As mentioned in the previous section the main stream way of accessing the data by programs is through Win32 API. Each program working in relation with registry, uses API where the whole function of this API is to retrieve the data from the required entry path and the name from the registry. For making any change to the content of the registry programs uses standard APIs which are compatible with the operating system.

Once the data is fetched using the APIs, the data is interpreted and implemented according to the functionality of the program. For instance if "1" is obtained as a result in the value it might means to enable or disable one particular feature of the program, which was previously operating other way. If in the value of the registry a file location is stored that might means that to save the program to the specified location or move the program to the specified location after the execution of the program.

In windows specifically the windows Server 2003 or higher Operating system the registry is used by the programs and the component of the operating system for the following purposes.

Setup: This includes the setup programs that

are for windows server 2003 or the setup program that are required for other hardware to be installed on the PC, the configuration is added to the registry e.g. every time new information is added to the registry when SCSI adapter is installed or the settings of the display are altered. Moreover, all the components are first read by the registry to ensure that all the prerequisite for installation are available.

Recognizer: Every single time when computer is turned on, the role of recognizer starts it puts the configuration of hardware data in the registry. The hardware configuration data includes the list of hardware that are available on system. The operation of hardware detection is carried out by windows kernel (Ntoskrnl.exe) programs and hardware recognizer (Ntdetect.com).

The role of the kernel program during startup of system is to ensure that the information related to the device is extracted from the registry this information includes the drivers that needs to be loaded and the sequence in which the drivers are supposed to be loaded. Another important feature of the kernel is reveal its own information to the registry, such as what kernel version currently it is, that's being used by the system.

Device Drivers:

The load perimeters along with configuration data is sent and received by the registry through device drivers. The role of the device driver is to report the information regarding the usage of system resources to the registry like the hardware interrupts or DMA channels that are utilized by one particular program. Registry information can be accessed by the device drivers or program so that smart installation and configuration can be provided to the user.

Since there is variability in programs, it is therefore very hard to know how a particular program will interpret the data of the registry. Registry entries are strictly dependent on program not the user, therefore one must not try to alter any registry entry of any program unless he/she is quite sure about the program.]

2.5 Users and the Registry:

For most of the programs today, there is hardly any need of user to go to registry for editing purposes for any particular task, from changing preferences to changing the features and services of program it is all done by the administrative tools and windows interface for the ease of the user. However, there are few rare cases where users has to go to registry settings to make changes to the instance of the operating system.

3. Windows Registry Forensics:

One of the essential steps that's being carried out in computer forensics is related to the analysis of the digital evidence, here at analysis stage different aspects are analysed which includes, the processes that are running on the ram when computer device was taken into custody, the files that are within the system and the files that were deleted, and windows registry analysis. [5]

When it comes to the analysis of windows registry it not only includes the viewing of data that is in registry, but it also involves the extraction and interpretation of data with respect to the context of investigation and with respect to its existence. Therefore, firm knowledge and understanding about the components of the registry is required. [3]

In the initial phase of the investigation several keys should be analysed. The key which should be examined includes the keys which

store the basic information related to the system, information related to the user, information related to the installed applications on the system, moreover, the information should include what drives were mounted on the system and what hardware components have been configured and installed on the system [6].

This process of analysis should be done in a proper sequence to make sure that the process of investigation is completed smoothly. The order of this investigation is as follow.

HKEY LOCAL MACHINE\Software:

In the preliminary phase of investigation, the most important thing is to know about the system and its owner. For digital evidence it is said that the more information that you get is more beneficial for you because it makes the analysis process easier. Before carrying out the forensics investigation it is mandatory to make sure about the directory and its path in which the windows operating system is installed and at same time it is important to know about the owner of the system. The HKEY LOCAL MACHINE\Software key has the information about the software that are installed on the system. Several keys are under this particular hive, the content of this hives can vary from system to system as everyone is not using the same software. Under this software hive there is a subkey of Microsoft\ Windows NT\Current Version subkey that is critically examined and special consideration is given to the data that is found within this particular subkey, because it contains important information related to the software installed, some of the important keys are as follow

- **CSDVersion:** The data that is found inside this value is related to the service pack installed. Windows boot loader use this key along with the **Current Version Key and Current Build Number key**: As every software or a patch has a build number or version so that it can be easily differentiated if it was created before certain time or after that particular time [7].

- **InstallDate**: As the name of the value suggest that this value has to do something with the time stamp which is very important in the forensics investigation, this particular value contains the information related to the date and time when the operating system was installed. The value is stored in Hex form. There are some tools that are used to decode this hex value for knowing the exact date and time when OS was installed, so that if the suspect has formatted the hard drive and has installed the windows again this could be determined.

- **PathName and SystemRoot**: The values within this subkey reference to the system directory. The default directory for system is %SystemDrive%:\Windows.

- **ProductID and ProductName**: The data within these values contains information related to the product key of the Microsoft product that is usually the one that's given as product key on the CD of Microsoft products. These values are the Microsoft product ID and a product name. Whereas the product name is simply the name of the operating system.

- **RegisteredOwner and Registered Organization**: Within these values the information that is stpred is related to the users and the organisation that is using these software in most of the cases it's the information of the actual owner of the software who is using theses software,

these values can be changed as it's under the control of the user every time a fresh installation process is carried out the program asks for the users details, which user has to enter.

- **NetworkCards**: The MAC address of network cards and the name of the particular network card linking to the MAC address is placed within this value. When the MAC address of the network card is deliberately changed during the course of hacking a new subkey is added, and from here we can investigate if the MAC address is changed.

HKEY LOCAL MACHINE\System

Once the information pertaining to the owner and system is gathered, the next step for the investigator(s) should be to check the configuration settings of the machine, and this is where we need to check HKEY LOCAL MACHINE\System hive, this hive maintains information related to the configuration setting that is required for booting the system and several other critical features required for the operations of the system. Some of the important subkeys that are within this hives are as follow [8].

Control:

The subkey of control has the information regarding the controls of the operating system with respect to its operations from booting of an operating system to the networking of the system to windows to windows on windows (WOW). Time zone, system boot date and time, with shut down date and time can be found through this subkey.

• **Enum:** This subkey has the information related to the hardware aspect related to the system, this includes the state of the hardware, legacy devices, and the long list continues. Moreover, settings related to the external storage devices are stored in this key. The accuracy of the information in this subkey is that it gives the exact name, and the model number of the storage device attached to the system. Now if the investigator further wishes to know when the device was installed, he can refer to the windows event log.

ControlSet001: It is one of the main control set, which is used by the default to boot the windows operating system.

ControlSet002: In case windows is unable to boot using controlSet001 this is backup control set which can be used. There are is possibility that there could be more than two numbered control set. There is a possibility that due to the variation in the registry Controlset002 may not appear but may be controlset003 appear as a backup control set. The setting of every control set may vary, so therefore it is highly recommended for an investigator to keenly observe the control setting of the Select subkeys.

Select:As cautioned earlier that if the investigator has to find out which control set setting are used at the boot of windows OS he must check the Select sub key. The role of this subkey in registry is to store information that a control set use to boot a computer. The select hive key contains the four subkeys, the Current, Default, Failed and the LastKnownGood. Among these 4 the current subkey is the one that has the value of the ID of current control set which is used for booting the windows. This is the reason it is important for an investigator to thoroughly check control set before examining the other configuration settings.

Mounted Devices:
The role of this subkey is to list the volumes/drives that have been attached to the system, because of this subkey one can determine the number of partition that were within the system and the auxiliary disks that were attached to the system inform of CD/DVDs drive or any other external medium like USB. This is another point at which the investigator should be cautious as this will show the investigator about the drives that are missing at the time of taking system image into the custody. [9]

HKEY LOCAL MACHINE \ System \ Control Set \ Enum:
Moreover, this Enum subkey contains information related to each devices, services, and drivers that might have been attached to system at any particular point. There are several services that an Enum entry may contain like entry of ATAPI driver even if there is no ATAPI interface on that machine. The purpose of these keys is to map devices and service to the relevant drivers and configuration on the system.

• **USBSTOR**: The role of this key is very significant and one of the most important role as it contains information about all the USB devices that has ever been attached to the system, even if it was not connected at the time of seizing the system. Each key has a subkey that contains the information about USB device such as the ID of the Hardware, Friendly name of the device and some other information related to USB the purpose of hardware ID and friendly name is to highlight the manufacturer name and model name. The moment when the forensics investigator figures out that the path of the file links to an external USB storage device, he should look into this subkey and should take appropriate steps, to know about the device(s) that were attached to the system [10].

Services\%AdapterGUID%\Parameters\Tcpip:
In case of attack related to the intrusion in the network or circulation of the malware within the network, this subkey is not less than a gem for the investigator as this subkey contains a lot of valuable information, as it contains the parameter linked to the TCP/IP network. The IPAddress mentioned in this subkey is the actual IP address that is allocated to the network adapter card. The Default Gateway contains the IP address of the gateway linked to the network.

4. Conclusion

Undoubtedly Windows registry has one of the important role in the forensics investigation of personal computers. As the components within the registry contains the important information related to the operations of the computers whether it is linked to hardware of the system, software of the system, drivers installed on the system, or the time stamp every aspect that is within the registry of the windows operating system is critical to the investigation. Just like in any other investigation where minimal things carry great importance [11] Windows registry forensics carries great importance as well.

5. Reference

[1] Harlan Carvey, “Windows Registry Forensics Advanced Digital Forensic Analysis of the Windows Registry”, Syngress Elsevier Inc, Burlington, pp 20, (2011).

[2] Khawla Abdulla Alghafli, Andrew Jones, Thomas Anthony Martin. 2010, “Forensic Analysis of the Windows 7

Registry", Edith Cowan University Research Online. Available at: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1071&context=adf

[3] Microsoft (2018), "Structure of the Registry", [online] Microsoft Windows Dev Center. Available at: https://docs.microsoft.com/en-us/windows/desktop/sysinfo/structure-of-the-registry

[4] Abhijeet Ramani, Somesh Kumar Dewangan (Nov 2014), "Digital Forensic Identification, Collection, Examination and Decoding of Windows Registry Keys for Discovering User Activities Patterns" International Journal of Computer Trends and Technology (IJCTT) volume 17 number 2–Nov2014. Available at: https://mafiadoc.com/ieee-paper-template-in-a4-v1_59f365cc1723dd8ee9ed8ea4.html

[5] Microsoft (2009), "Overview of the Windows Registry", [online] Microsoft Windows Dev Center. Available at: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc781906(v=ws.10)

[6] Yang, S., Wang, L., Zhang, S., & Liu, J. (2013). "A Method on Extracting Registry Information from Windows CE Memory Images", 2013 International Conference on Computer Sciences and Applications. Available at: https://ieeexplore.ieee.org/document/6835701

[7] Saidi, R. M., Ahmad, S. A., Noor, N. M., & Yunos, R. (2013). "Windows registry analysis for forensic investigation." 2013 The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE). Available at: https://ieeexplore.ieee.org/document/6557209

[8] Chang, K., Kim, G., Kim, K., & Kim, W. (2007). Initial Case Analysis Using Windows Registry in Computer Forensics. Future Generation Communication and Networking Available at: https://ieeexplore.ieee.org/document/4426183

[9] Shuhui Zhang, Lianhai Wang, & Lei Zhang. (2011). Extracting windows registry information from physical memory. 2011 3rd International Conference on Computer Research and Development. Available at: https://ieeexplore.ieee.org/document/5764089

[10] Deb, S. B., & Chetry, A. (2015). "USB Device Forensics: Insertion and removal timestamps of USB devices in Windows 8." 2015 International Symposium on Advanced Computing and Communication (ISACC). Available at: https://ieeexplore.ieee.org/document/7377371

[11] Dr Aftab Ahmed Malik, International Journal For Electronic Crime Investigation (IJECI) Volume 1 2017. Available at: http://lgu.edu.pk/dfrsc/journal/Journal-IJECI.pdf