ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Windows Recent View-Tracking recent activities- Cyber Forensics

[1]Soji Joy, [2]RajKumar T, [3]Sobhana N V

[1]*Dept of Computer Science, College Of Engineering Kallooppara Pathanamthitta, Kerala, India.*
[2]*Dept of Computer Science, College Of Engineering Kallooppara Pathanamthitta, Kerala, India.*
[3]*Dept of Computer Science, Rajiv Gandhi Institute of Technology Kottayam, Pampady, Kottayam, Kerala, India.*

ARTICLE INFO

Article history:
Received 1 December 2015
Accepted 31 December 2015
Available online 10 January 2016

Keywords:
Cyber Crime; Cyber Forensics;Registry;User Assist;Log;Prefetch;Windows7;Recent Activity;

ABSTRACT

Computers and the Internet made our lives easier in many ways, but it is unfortunate that people also use these technologies to take advantage of others. Today's society relies heavily on computers and the internet to accomplish everyday tasks,which mightincludes everything practically from communicating and shopping online to banking and investing.Along with the increasing use of computers and the internet, comes some amounts of problem called computer crime. Computer crimesincluding, but certainly not limited to fraud,phishing, identity theft, network infiltration, and piracy of copyrighted material. With computer crimes on the very high rising rate, it is becoming extremely crucial for law enforcement officers and digital forensic examiners to understand computer systems and be able to examine them efficiently and effectively. In order to do this, they must have good knowledge of the System and how to discover the activity information from the system. The Registry is the heart and soul of the Microsoft Windows operating system and an exponential amount of information can be derived from it. We can say, everything done in Windows refers to or is recorded into the Registry.This paper will introduce the locations for tracking recent activities in a Windows 7 machine for cyber forensic investigation.We can gathers information from various sources, such as the registry, the events log of Windows, Prefetch, UserAssist, Recent locations of Windows and other sources.In essence, the paper will discuss various sources of activity 'footprints' and describe many of the Registry keys that are imperative and relevant to an examination.

To Cite This Article: Soji Joy, RajKumar T, Sobhana N V., Windows Recent View-Tracking recent activities- Cyber Forensics. ***Aust. J. Basic & Appl. Sci.,*** *9(36): 503-508, 2015*

INTRODUCTION

Cyber Crime is any crime that involves or committed with a computer or other digital device. Two Categories of Cyber Crime

- Crimes committed against a computer
- Crimes committed by taking the help of a computer

Cyber-crime sections are more watchful and taking assistance of latest software and tools to get the cases crack down. Computer forensic is the application of investigation techniques to preserve evidences from a particular computing device in a suitable method for presentation. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and reports the facts and opinions about the digital information.

Computer forensics helps to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

The Registry was first introduced with Windows 95 and has been incorporated into many Microsoft operating systems since. Although some versionsare slightly differ, they all are specifically composed of the same structure and serve the main purpose as a configuration database. The Registry replaces the configuration files that were used in MSDOS, like config.sys and autoexec.bat. The main purpose of config.sys was to load device drivers and the use of autoexec.bat was to run startup programs and configure environment variables. Registry now handles these functions in an efficient manner. Registry replaces DOS configuration files, moreover it also replaces text-based initialization (.ini) files that were introduced in Windows 3.0. The .ini files - specifically win.ini and system.ini - store user settings and operating system parameters. Registry is the central hierarchical database used in Microsoft Windows, used to store information that is essential

Corresponding Author: Soji Joy, Dept of Computer Science, College Of Engineering Kallooppara Pathanamthitta, Kerala, India.
E-mail: sojijoy333@gmail.com

to configure the system for multiple applications, multiple users and many devices.

Collecting Evidence from Registry:

Registry is the central database of Windows systems, used for getting system information, establish time lines of activity , USB Devices, list of applications and file names of the most recent files opened in windows , user application data etc. We can view our Registry via REGEDIT and it appears to be just a bunch of settings, but Registry keys have a little more to them. And the most interesting additional feature is a "last written" time, which reveals you when a particular key (though not a value) was written.

If any of your programs write to the Registry when you have used them,for instance, and those write times will reveal which applications you were using, when, and maybe even over some clues as to how you were using them (depending on which area of the Registry had been changed). The Registry will be always updating its timestamps when keys are rewritten.

The Windows Registry is a data repository that exists on each computer in Windows operating systems. Both the system and application programs use this repository to store information needed at runtime. The system reads the Registry into memory at bootup. This memory image then serves as a working copy for the system. When the system is shut down, it persists the current Registry to disk. The Registry is stored in various files. Based on the version of Windows, the location and organization of these files may vary. For example, in Windows 2000, the Registry is stored in a number of files located in the %SystemRoot%System32Config folder, whereas in Windows 95, the Registry is contained in user.dat and system.dat, the hidden system files in the Windows folder. In all cases, those files can not be edited directly. Changes to the Registry can be made only programmatically or by using a special Registry editor application.

Structure of the Registry:

The Windows Registry is depicted as one unified file system. It mainly contains five hierarchical folders. Those five main folders are called hives,and begin with HKEY (Handle to a Key.) Each of these hives[1] is composed of keys that contain values and sub keys. Values are the names of items that uniquely identify specific values applicable to the OS, or to applications that depend upon that value. The keys depend on folders and sub keys depend on sub folders of Windows Explorer.

A. Hkey_Classes_Root (Hkcr):

Information stored here ensures that the correct program opens when it is executed in Windows Explorer. It also contains other details on rules of drag-and-drop, information on the user interface, and shortcuts.. Alias for: HKLM\Software\Classes

B. Hkey_Current_User (Hkcu):

Contains configuration information for the user who is currently logged into the system, which includesscreen colors, user's folders, and Control Panel settings. The generic information usually applies to all users and is HKU\.DEFAULT. Alias for a user specific branch in HKEY_USERS.

C. Hkey_Local_Machine (Hklm):

Contains machine hardware-specific information that the operating system runs on. It contains a list of drives mounted on the system and generic configurations of installed hardware and applications.

D. Hkey_Users (Hku):

It stores configuration information required for all user profiles on the system, which concerns application configurations, and visual settings.

E. Hkey_Current_Config (Hcu):

Stores configuration information about the current system. Alias for: HKLM\Config\profile

F. Registry structure inside Hive:

Inside the registry, various types of cells are there and they are:

- Key Cell - This cell contains Registry key information and includes offsets to other cells as well as the LastWrite time for the key (signature: kn).
- Value cell - This cell holds a value and its data (signature: kv).
- Subkey list cell - This is a cell made up of a series of indexes (or offsets) pointing to key cells; these are all subkeys to the parent key cell.
- Value list cell - This is a cell made up of a series of indexes (or offsets) pointing to value cells; these are all of the values of a common key cell.
- Security descriptor cell - This is a cell that contains security descriptor information for a key cell (signature: ks).

Registry Forensics:

Registry keys contain a value called the LasWrite time, which is very similar to the time of the most recent file modification. The value is stored in a FILETIME structure and it represents the last modification of a Registry key. The LastWrite time is changed when a registry key has been created, accessed, modified or deleted. Unfortunately, only the LastWrite time of a registry key can be obtained, when as a LastWrite time for the registry value cannot. Information on the LastWrite time of a key can allow a forensic analyst to infer the approximate date or time an event occurred.

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”.

G. Software Uninstall Registry Key:

The Software Installation details have to taken from the following registry keys

- *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall*
- *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall*

H. Collecting Evidence from UserAssist:

Every time you run a program, Windows records details of that particular session under a Registry key named User Assist. This list can extend for a very long time: they don't just record the last 20 applications, ratherit may can 1,000 or more listed. There exist a "Last used" date, most important data for an investigator, and the number of times a program has been run, so at a glance an investigator could see which applications

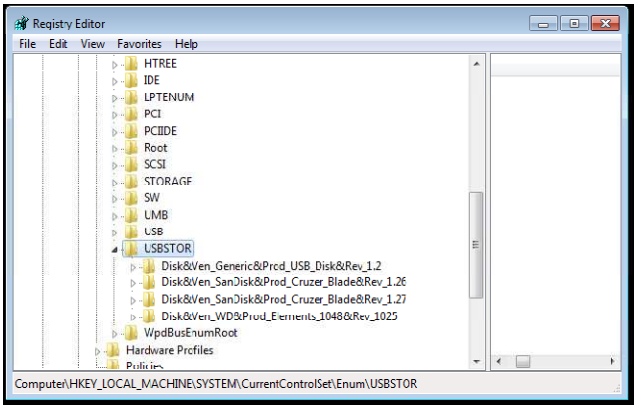

Fig. 1: Storage Device Entry in Registry

you have used most often. UserAssist is a method used to populate a users start menu with frequently used applications. This can be obtained by maintaining a count of application use, for each users NTUSER.DAT registry file. The data about frequently used programs, usually keptunder this key in the registry:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

Beneath each Count key are several values;in fact, there might be many, many values. To a degree, these keys actually record user activity like a log file. One of the benefits of parsing the contents of the UserAssist key is that, it not only shows what actions the user took through the shell (e.g., double-clicking icons, launching an application through the Start menu, or accessing Control Panel applets), but also shows the time at which these actions occurred.

I. Most Recent Used (Mru):

1) Open/Save MRU list in the Registry:

Every time that we choose a filename in a standard open/save dialog-box of Windows, a new entry is added in the Registry under the following key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

As The contents of this key can be very useful in several ways. Firstly , some file extensions will not appear frequently during normal system use, so the sub key beneath the OpenSaveMRU key for that file extension may have only one entry.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

OpenSavePidlMRU key maintains MRU lists of files opened via the Open and Save As dialogs within the Windows shell. The OpenSaveMRU key also maintains sub keys of specific file extensions that have been opened or saved.

2) Run MRU:

In Windows Registry, we could find many keys with a suffix MRU.

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

The above mentioned key stores the information in the “run” command drop down list. Based on 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 a suspectsystem, according to the commands the intruder entered and the timestamps, the investigator may be able to decide what the intruder did and when.

3) Recent Docs:

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

Recent documents access is very useful to view the recently opened files from a local computer or from a network location. Most often you would have opened and worked with a file, but forgot the exact location of it, you can easily find your particular important files by viewing the recent documents list, no matter where its saved. Every time that you open a file, automatically a new shortcut to this file is added to the recent folder of Windows. Corresponding location in Windows is :

C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Recent

J. IE explorer Typed URLs:

- HKEY_USERS\S-1-5-21-3991512384-2868679077-3788496241-1000\Software\Microsoft\Internet Explorer\Main
- HKEY_USERS\S-1-5-21-3991512384-2868679077-3788496241-1000\Software\Microsoft\Internet Explorer\TypedURLs

The first Key stores the user's settings, search bar information, start page, etc. The second Key storestyped URLs entered into the address field. The last typed URL is "url1" and the first typed URL is "urlx" where "x" is the highest number in the list.Recently typed urls in the address field of Internet Explorer will be obtained from the Typed URLs field.

- HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\TypedURLs

K. Searches:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ WordWheelQuery

When searching for files or folders using Windows Explorer, this Key will store the search query. This piece of information will also help the investigators to conduct further actions.

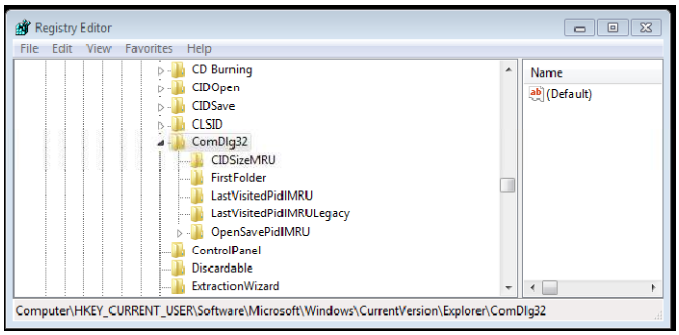

Fig. 2: Open/Save MRU Entry in Registry

L. Typed Paths:

Whatever url or path pasted in the windows explorer can be obtained from the following key. It will help the investigator to identify the path or folder or file the suspect has been trying to use.

- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

M. Attached Device Information:

1) Storage devices:

Windows is particularly good at tracking hardware use. And this can have its own advantages. Suppose if you run a business, and someone try to plugs in a USB ash drive to a company workstation, then tried to copy some confidential files across, they would think their crime has left no trace: but that would be a mistake.

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

The reality is that Windows always maintains details on every USB device which connects to your PC, and when the last connection was made.

Anytime a device is connected to the Universal Serial Bus (USB), drivers are queried and the device's information is stored into the Registry (i.e., thumb drives). This key stores the contents of the product and device ID values of any USB device that has ever been connected to the system. Beneath each device name is the Device ID, which is the serial number. The serial numbers of such devices are a unique value assigned by the manufacturer, similar to the the MAC address of a network interface card (NIC). This way, a particular USB device could be identified to determine whether or not it has been connected to other Windows systems. The Windows Registry as a Forensic Resource, an important consideration have to keep in mind regarding USB device IDs. Every thumb drive need not have a serial number. Particularly, those that have an '&' symbol for the second character of the device ID. However, if the '0' was an '&' that would indicate to an examiner that the device doesn't have a designative serial number. Knowing what USB devices have been connected to a system can assist an examiner in

collecting additional evidence that may be crucial to the investigation.

2) Mounted Devices:

There is a key in the Registry that makes it possible to view each drive associated with the system. The corresponding key is

- HKLM\SYSTEM\MountedDevices

and it stores a database of mounted volumes that is used by the NTFS file system.This information can be useful to a digital forensics examiner as it shows the hardware devices that should be connected to the system. So, if a device is shown in the list of MountedDevices and that device isn't physically in the system, it might indicate that the user removed the drive in attempt to conceal the evidence. In such case, the examiner would know they have additional evidence that needs to be seized.

Collecting Evidence From Prefetch:

Whenever you execute a program on your Windows machine, Windows will notes the associated files and areas of your drive that are accessed, and then on a later time, if you again execute the same program, it preloadsthese files, so your apps start more quickly. Prefetch file contains the name of the application, then a dash and then an eightcharacter hash of the location from which that application was run, and a.pfextension. The filenames should be all uppercase except for the extension. Ifan application is run from two different locations of the drive, there will be two different prefetch files in the Prefetch folder. Recently executed applications details can be obtained from this source.

Collecting Evidence from Web Browser History:

Web History will provide more information to the cyber forensic investigating officer. The most characteristic of forensic data on a system, what you lookfor as evidence actually depends on the nature of your case. You could find references to sites from which malicious software tools may be downloaded or otherwebsites, the user browsing. However, nothing should be overlooked; small bitsof information can provide clues or context to your evidence or to the case as awhole.

Collecting Evidence from Services:

Evidence from the services installed on the systemwill provide valuable information to the Investigator.All services are need not be installedby the user or even by the system administrator.Most probably, malware installs itselfas a service or the attacker can install a malicious service on the system. In such cases, analyzing installed service details will help the investigator.

Collecting Evidence from JumpLists:

Windows 7 introduced a new feature Jump Lists, proper shortcutswhich appear when you right-click a taskbar button. Just like Prefetch files, theseare generally a good feature. If you like to reopen a recent document in Word, there's no need to go to the application menu: just right-click its taskbar button and choose your file from the list. This source of information will enable the investigator to identify the files opened by each applications. You'll find jumplist at%APPDATA%\Microsoft\Windows\Recent\CustomDestinationsand% APPDATA% \Microsoft \Windows \Recent \AutomaticDestinations.

Collecting Evidence from Event Logs:

Event logs are special files that record significant events on your computer, when a user try to logs on to the computer or the system is going to shut down. Whenever suh types of events occur, Windows records these types of data in an event log that you can read by using Event Viewer. Users might findthe details in event logs helpful when troubleshooting problems with Windows andother programs. Cyber forensic investigators can properly collect evidences related to System start, System shutdown, User Logon, User logoff, software crash and similar activities from these event logs.

Conclusion And Future Works:

This paper gives an overview of the important recent activity sources of Windows 7, that has a significant role in cyber forensics investigation process. This will help the Cyber Forensics Experts to easily collect evidence from the Windows7 system.Collecting data from these locations may be crucial for proving someone's guilt or theirinnocence.In future,new versions of Windows OSes will have additional features,that will open ways and means to probe into such matters or activities more effectively.

REFERENCES

Lianhai Wang, Hengjian Li, 2011. "E_ect of Live Evidence Acquisition Process on the change of Windows XP SP2 Registry S2012" International Workshop on Information and Electronics Engineering (IWIEE), Elsevier Ltd

Kris Harms, 2006. "Forensic analysis of System Restore points in Microsoft Windows XP" Digital Investigation,Elsevier Ltd, 4(34): 151158.

Saidi, R.M., S.A. Ahmad, N.M. Noor, R. Yunos, 2013. "Windows registry analysis for forensic investigation", IEEE, Technological Advances in Electrical,Electronics and Computer Engineering (TAEECE), 132-136.

Thomas Schwarz, "Windows Registry Analysis, Computer Forensics 2013"www.cse.scu.edu/tschwarz/Windows%20Registry%20Analysis.pptx

Elizabeth Schweinsberg "Taking Registry Analysis to the Next Level"

https://digitalforensics.sans.org/summit-archives/2012/taking-registry-analysis- to-the-next-level.pdf

Harlan Carvey, Eoghan Casey, 2009. "Windows Forensic Analysis" Registry analysis,File Analysis, 157-252: 253-298

Access Data Corporation, 2008. "Understanding the UserAssist Registry Key", pp: 1-16.

Mark Wade, 2010. "Decoding Prefetch Files for Forensic Purposes",www.forensicmag.com/prefetch-_les-forensic-purpose-part-1

Chad Tilbury, 2010. "OpenSaveMRU and Last Visited MRU" http://digitalforensics.sans.org/blog/2010/04/02/open runsavemru-lastvisitedmru/

Joachim Metz 2011-2014. "Windows Prefetch File(PF) Format"