ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

RegAnalyzer Tool to Automate Windows 7 Registry Forensics Analysis

Sameer H. Mahant[*1], Dr. B.B.Meshram[2]
Department of Computer Engineering
Veermata Jijabai Technological Institute,
Matunga, Mumbai, Maharashtra, India
shm.mtech@gmail.com[1]
bbmeshram@gmail.com[2]

Abstract: Use of computers for performing crimes is increasing day by day. It has become necessary for investigator to collect evidences from suspect's computer. Windows 7 has become mainstream operating system for users and thus its forensics investigation is becoming important. One of the areas of interest is windows registry. It contains valuable information that can be helpful for the forensics analysis. Registry contains the basic information like date when Operating System installed, owner name and the advanced information such as the software and hardware devices installed on system, storage devices attached to system, services running on system, history of recently used documents and so on, which will help the analyst to decide the way of further analysis of system depending on the its environment. Though it has such valuable information it is very difficult for an analyst to manually search and analyze it to collect evidences because of its complex structure. So in this paper we presented details of Windows 7 registry, its use for forensic analysis and proposed design for a tool (RegAnalyzer) which will automate task of windows 7 registry analysis for forensics investigator so he/she can use it for the further investigation of system.

Keywords: computer forensics; registry forensics; registry structure; windows 7 forensics; windows registry

I. INTRODUCTION

Windows operating systems are used by most of the home users and by the organizations for its user friendliness. Launch of Windows 7 has increased this percentage as it is more robust and secure operating system that its previous versions, becoming the mainstream choice of operating system for users. The concept of registry is used by Microsoft's Windows XP, Vista and also in Windows 7 operating system for storing configuration data and user setting; but its complexity has increased much more in its evolution. Almost for each user's activity on computer registry is referenced one way or another.

Suspect's activities on windows 7 computer and application software used by suspect may leave behind the tracks within the Registry that can help the investigator. So it is important for investigator to have knowledge of this operating system and its registry. But due to registry's complex structure it is very difficult and time consuming to extract required evidences. Keeping this need in mind we proposed a design of tool *(RegAnalyzer)* which will automate task of windows 7 registry analysis for forensics investigator.

This paper will describe the structure and organization of registry in windows 7 operating system, some locations in registry which are important in forensic analysis, design of tool to automate registry forensics.

Windows 7 registry structure, registry data types, five registry hives and their relation with files on disks is discussed in Windows Registry section. Forensic Analysis of Registry section describes importance of some registry locations in forensic investigation. A design for tool (RegAnalyzer) is given which will help to automate registry forensic investigation.

II. RELATED WORK

Windows Registry is gaining importance in computer forensic analysis as various researchers working on it and finding information from it that can be put forward as evidences of user's actions on windows system.

Information stored by any program will be located either in a file or within the system registry. It is a forest of digital evidence. Its Basic features and common applications are discussed by Fauzan Mirza in his paper. [1]

Impact of Windows 7 on Forensic Examination and the details of notable changes in Windows 7 registry files, registry hives and their associated file paths are given in the paper. [2]

Muhammad Yasin presented the traces of Download Accelerator Plus software in registry and their use in forensic investigation. [3] The artifacts of Skype software is documented by Ronald Dodge. [4]

Brendan Gavitt in his paper describes the structure of the Windows registry as it is stored in physical memory and presented tools and techniques that can be used to extract this data directly from memory dumps. [5]

Zhenhua Tang has given a carving algorithm for the registry files based on the registry file internal structure. [6]

Paul McFedries in his book described how to work with Registry Editor which is a default tool provided by Windows operating system. How registry settings affect the computer environment. [7]

All of above work helped to get good knowledge of windows registry, its structure and its importance in computer forensics analysis.

III. WINDOWS REGISTRY

The registry is a system-defined database in which applications and system components store and retrieve configuration data. The data stored in the registry varies according to the version of Microsoft Windows. [8] Windows registry is a central repository for all information that is required for the settings and configuration of windows system, hardware and users, arranged in a hierarchical structure.

It includes some of following information and much more:

i. Information about systems environment such as windows installation directory, location of program files & documents folder
ii. Settings of third-party applications installed in the system
iii. Hardware devices attached to the system
iv. List of programs and device drivers that windows load and run on the startup of system
v. Username and password of the account used for auto login into windows
vi. List of recently executed commands from 'Run' menu, recently opened documents

Thus using the registry forensic investigator can get lot of information about the suspect's machine.

A. *Registry Structure:*

In this section we will describe the structure of the registry and registry data types with description that will be helpful in understanding registry.

The registry is a hierarchical database that contains data that is critical for the operation of Windows and the applications and services that run on Windows.

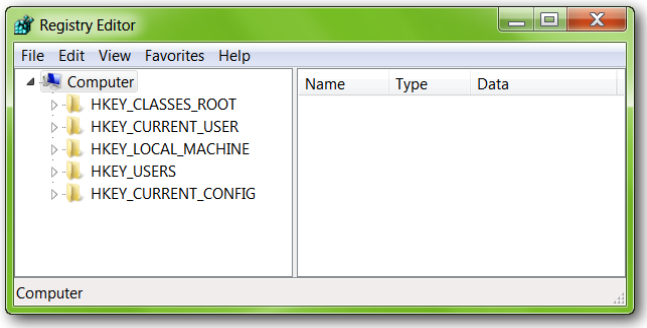

Figure 1: Windows 7 Registry

The data is structured in a tree format. Each node in the tree is called a *key*. Each key can contain both *subkeys* and data entries called values. Windows registry supports following three basic data types for registry values:

i. BINARY
ii. DWORD
iii. STRING

Registry also contains variations of these basic data types. Different data types are explained below:

a. ***REG_BINARY:*** Contains Binary data i.e. in the form of 0 & 1. E.g. 10001010
b. ***REG_EXPAND_SZ*:** is an expandable data string that permits storing of variables that can be replaced by actual value. For example: %ProgramFiles% will get expanded to "C:\Program Files".
c. ***REG_SZ:*** is used to represent normal string values that are in human readable form
d. ***REG_MULTI_SZ:*** Multiple values are stored as a list using this data type. NULL character is used to separate each value. Two NULL characters are used to specify end of list.

All the keys that end in '_SZ' are string values

e. ***REG_DWORD:*** It is mostly used to store Boolean values. It is 4byte number. It can be in Big Endian or Little Endian form. In Big Endian form most significant bytes are stored in the memory first. In Little Endian form least significant bytes are stored first. Intel architecture uses Little Endian format.
f. ***REG_NONE:*** It is used to represent values with no defined type.
g. ***REG_FULL_RESOURCE_DESCRIPTOR:*** Resource lists required by the physical hardware device are stored in the format of nested array. Plug and Play feature requires values of this data type. We can only see these values but cannot create this type of values using Registry Editor. Example: HKLM\HARDWARE\DESCRIPTION \Description
h. ***REG_RESOURCE_LIST:*** It contains a list in which values of REG_FULL_RESOURCE_DESCRIPTOR data type are stored.
i. ***REG_RESOURCE_REQUIREMENTS_LIST:*** Resources required by device are stored in list format using this data type.
j. ***REG_LINK:*** It is used to link key. User cannot create REG_LINK values.
k. ***REG_QWORD:*** Quadruple-word values (64 bits). This type is similar to REG_DWORD but contains 64 bits instead of 32 bits. It also has two variations like REG_DWORD : **REG_QWORD_BIG_ENDIAN and REG_QWORD_LITTLE_ENDIAN**

B. *Windows 7 Registry Organization:*

There are five *root keys* in Windows 7 registry as shown in Fig1. The root keys and their standard abbreviation are given in following table:

Table 1: Windows 7 root keys

Abbreviation	*Original Key name*
HKCR	HKEY_CLASSES_ROOT
HKLM	HKEY_LOCAL_MACHINE
HKCU	HKEY_CURRENT_USER
HKCC	HKEY_CURRENT_CONFIG
HKU	HKEY_USERS

The information contained in five root keys is given below:

a. ***HKEY_CLASSES_ROOT:*** HKCR hive stores the information about the file extensions (used to get information of file type) and applications associated

with that file type. It also stores information of objects that exists in windows 7.

b. ***HKEY_CURRENT_USER:*** HKCU hive contains the user specific information which includes Volatile Environment details, software installed for user, printer settings, network related details and more.

c. ***HKEY_LOCAL_MACHINE*:** HKLM hive stores the hardware and software settings as well as the security settings for the system. [3] This machine specific information directly correlates to the machine the operating system is run on. It includes lists of the drives mounted, hardware present and the generic configuration of installed applications.

d. **HKEY_USERS:** HKU is having information about preferences of user. Users are uniquely identified by SID (Security Identifier). If user is deleted and created again with same name, then also it will have different SID. It has configuration information for all system users.

e. **HKEY_CURRENT_CONFIG:** HKCC points to HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\####, where #### is number starting with 0000. It has information on the current hardware configuration.

In the above five root keys HKLM and HKU has more importance in forensic analysis and only these keys are store on hard disk by windows.

i. HKCR is having pointer to the subkey HKLM\SOFTWARE\Classes.

ii. HKCC is having pointer to the subkey HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current

iii. HKCU is the pointer to subkey HKU\SID, where SID is the unique id of current user.

Fig. 2 illustrates relation among Registry keys.

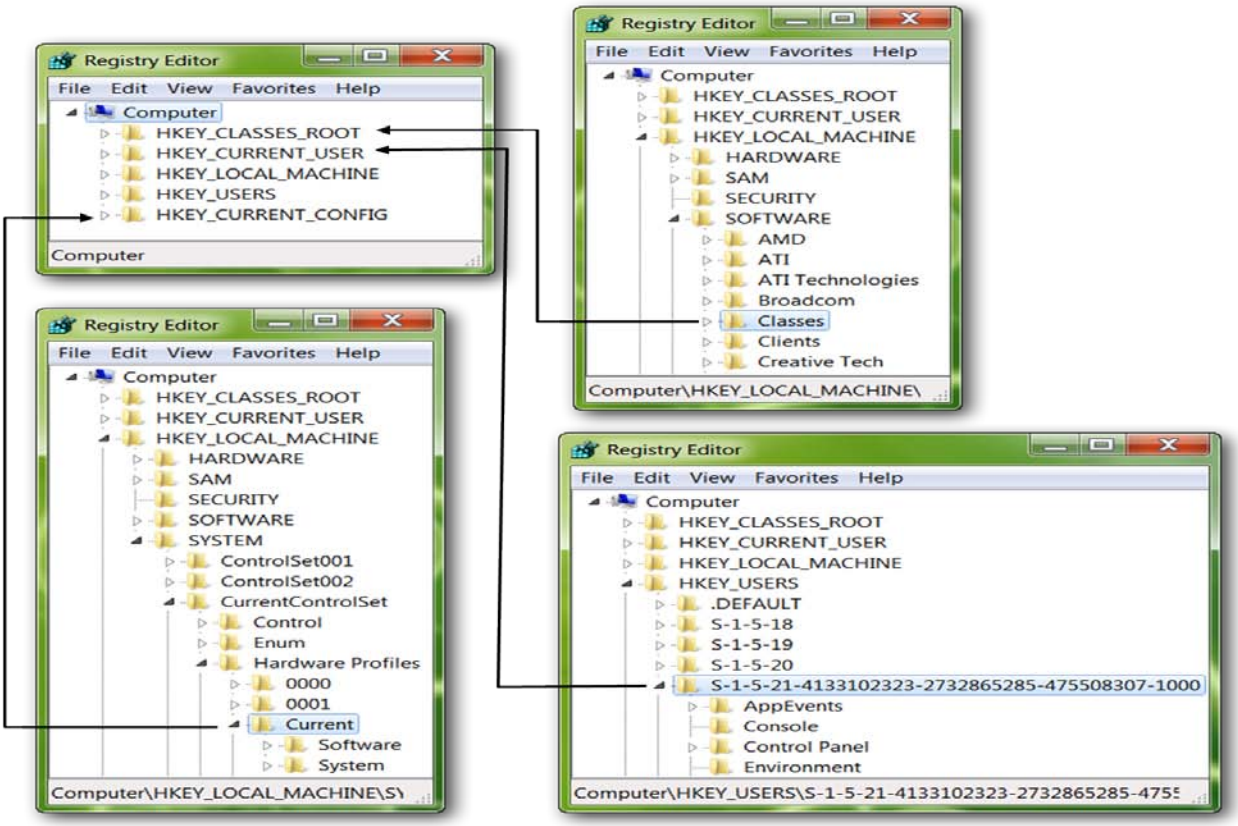

Figure 2: Relation of root keys with their links to subkeys

C. Relation of Registry Hives with files on Hard Disk:

The Registry database actually consists of a number of files that contain a subset of the Registry called a *hive*. A hive consists of one or more Registry keys, subkeys, and settings.

Each hive is supported by several files that use the extensions listed in Table 2. [7]

Table 2: Registry Hives extensions

Extension of File	***Description***
None	It is a complete copy of the registry hive contains.
.log1	Any changes made to hive are stored in the file having .log1 extension.
.log, .log2	During setup of Microsoft's windows 7 these files are get created and does not change when working with the system.

Location of files supporting each registry hive is given in Table 3 assuming default %SystemRoot% directory is located at 'C:\Windows\':[7]

Table 3: Location of files supporting Registry Hives

Hive	Files Location
HKEY_LOCAL_MACHINE\BCD00000000	C:\Windows\System32\config\BCD-Template C:\Windows\System32\config\BCD-Template.LOG
HKEY_LOCAL_MACHINE\COMPONENTS	C:\Windows\System32\config\COMPONENTS C:\Windows System32\config\COMPONENTS.LOG C:\Windows\System32\config\COMPONENTS.LOG1 C:\Windows\System32\config\COMPONENTS.LOG2
HKEY_LOCAL_MACHINE \SAM	C:\Windows\System32\config\SAM C:\Windows\System32\config\SAM.LOG C:\Windows\System32\config\SAM.LOG1 C:\Windows\System32\config\SAM.LOG2
HKEY_LOCAL_MACHINE \SECURITY	C:\Windows\System32\config\SECURITY C:\Windows\System32\config\SECURITY.LOG C:\Windows\System32\config\SECURITY.LOG1 C:\Windows\System32\config\SECURITY.LOG2
HKEY_LOCAL_MACHINE \SOFTWARE	C:\Windows\System32\config\SOFTWARE C:\Windows\System32\config\SOFTWARE.LOG C:\Windows\System32\config\SOFTWARE.LOG1 C:\Windows\System32\config\SOFTWARE.LOG2
HKEY_LOCAL_MACHINE \SYSTEM	C:\Windows\System32\config\SYSTEM C:\Windows\System32\config\SYSTEM.LOG C:\Windows\System32\config\SYSTEM.LOG1 C:\Windows\System32\config\SYSTEM.LOG2
HKEY_USERS\.DEFAULT	C:\Windows\System32\config\DEFAULT C:\Windows\System32\config\DEFAULT.LOG C:\Windows\System32\config\DEFAULT.LOG1 C:\Windows\System32\config\DEFAULT.LOG2

IV. FORENSIC ANALYSIS OF REGISTRY

In this section we have described how windows 7 registry can be a candidate for collecting evidences by giving locations in the registries where the investigator can look for related information.

Harlan Carvey highlighted importance of registry locations by saying 'Knowing where to look within the Registry, and how to interpret what you find, will go a long way toward giving you valuable insight into activity that occurred on the system'.[9]

A. LastWrite Time for Registry Keys:

Like files have attributes to determine the modification time of file, Registry key also has a attribute 'LastWrite' that determines when the registry key is modified.

FILETIME structure is used to store this value. Microsoft Knowledge Base describes that this structure represents the number of 100 nanosecond intervals since January 1, 1601.

Whenever we create new key, modify existing key LastWrite gets updated. We can obtain LastWrite time of a Registry key, but the old value cannot be obtained.

LastWrite time can be used by forensic analyst to create timeline of events like when some command is executed, USB drive has used, etc. It can be treated as a LOG of events when it is related to other file attributes like modified, accessed and created.

For Example: The W32/Opanki worm, as identified by Network Associates, installs a rootkit component, creating two Windows services (in addition to a number of other artifacts). Because most compromises occur sometime after the operating system is installed, sorting the Services keys based on their *LastWrite* times will often quickly reveal the issue. This is a useful technique for locating any of the myriad bits of malware that create Windows Services when they infect a system. [9].

B. Information about Operating System:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName contains the machine name given to the system which is seen over network.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion key contains the information about OS name; install date, its digital product id which is related to product key, service pack version, etc. Information which can be obtained from registry about operating system is displayed in Fig 3. Forensics analyzer can now continue its analysis based on the specific version of operating system.

For Example: Investigator can use service pack information to prove or deny the fact that machine is compromised by an attacker using some vulnerability in the operating system. If system is having latest service pack installed and have patched that vulnerability, investigator can prove that the system is not compromised by that vulnerability, but attacked by some other way.

Two important keys from this part are **RegisteredOwner** and other is **RegisteredOrganization** because most of the applications like Microsoft Office use this information in the file properties when creating document as author. These values can be used to prove the ownership of computer system.

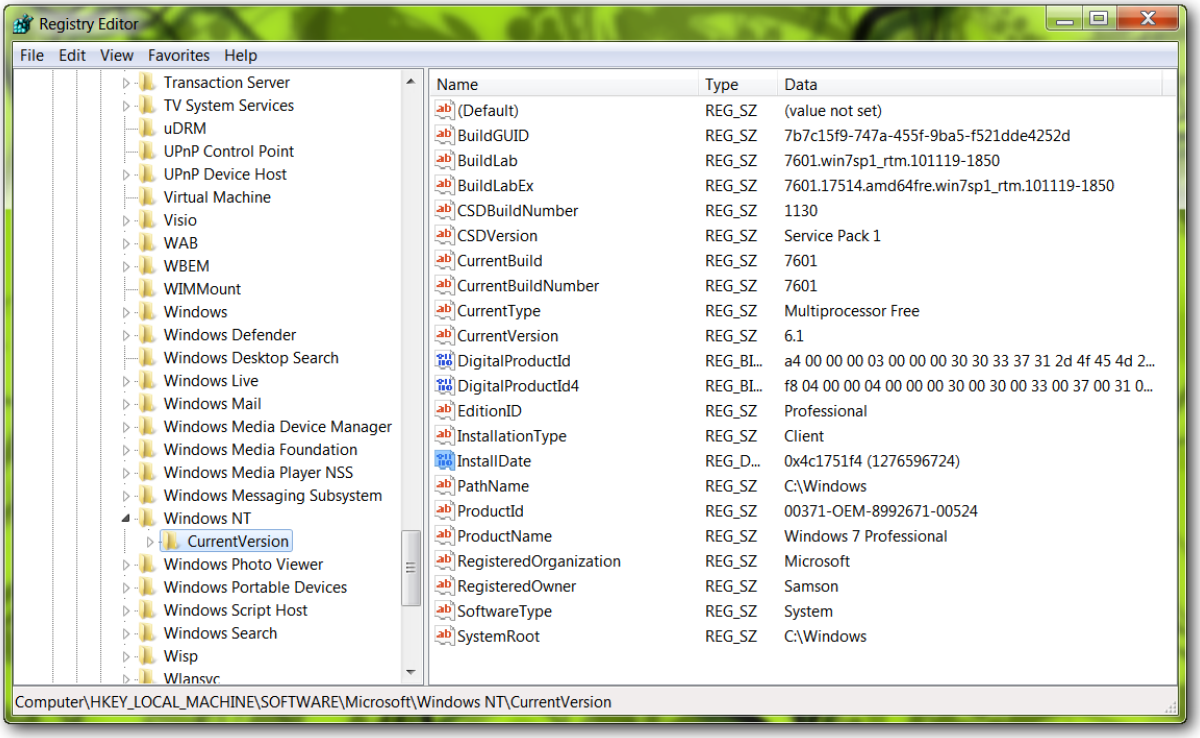

Figure 3: Initial OS information from registry

C. Time Zone Information:

Information about the time zone settings in the following key:

SYSTEM\CurrentControlSet\Control\TimeZoneInformation

This information can be extremely important for establishing a timeline of activity on the system. Extracted information regarding times and dates in UTC/GMT time, can use the *ActiveTimeBias* (listed in minutes) value from the TimeZoneInformation key to translate or normalize the times to other sources from the system, such as entries in log files.[9]

D. Network Interfaces Information:

Information about network interfaces, or network interface cards (NICs), is maintained in both the Software and System hive files. Within the Software hive file, the following Registry key contains information about network cards:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\10

E. MAC Address:

Media Access Control (MAC) address is the address of NIC, which is hardcoded into a NIC. To get the MAC address Windows operating system will first check a Registry key for address and then query the Network Card if it cannot get the address from registry.

Windows checks the value of '*NetworkAddress*' in the following key:

HKLM\SYSTEM\ControlSet00x\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\000*n*

In this Registry key, "000*n*" is the number of the adapter. This value can help forensic investigator to verify if the MAC address is changed by user for malicious purpose.

F. Auto Starting Programs:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run contains information about programs which starts automatically when you log into windows is shown in Fig 4. This location is very important as most of the viruses and worms use this for triggering themselves at each startup. Forensic investigator can check *LastWrite* time of this key to get the approximate time when the system was infected by malicious program.

G. Recently Executed or Opened Files:

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

This key maintains list of files recently executed or opened through Windows Explorer. On live system this is very useful to get information of documents on which user is working or recently worked.

H. RUN Command History:

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. Using this key and its LastWrite time forensic analyst can approximate the date and time for particular event.

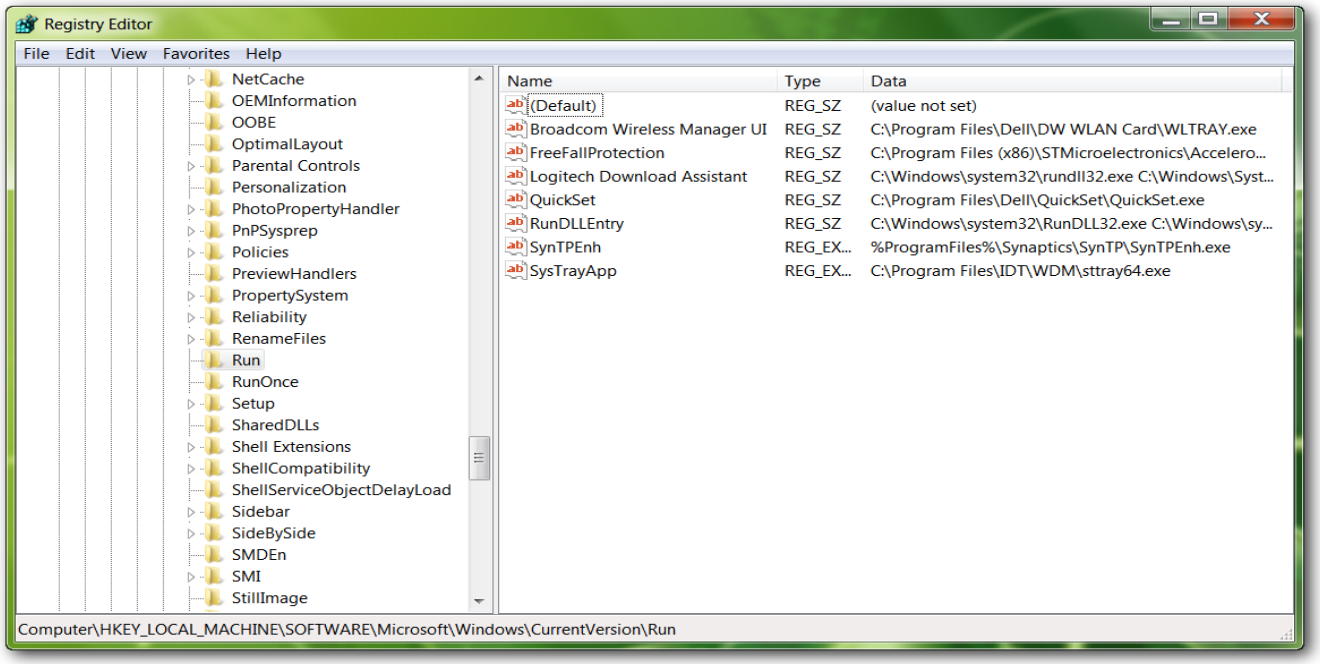

Figure 4: Auto starting Programs

I. Protected Storage:

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 PassView and PStoreView.

J. Information About USB Devices:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR contains information about USB devices connected to system. Fig 5 illustrates this fact.

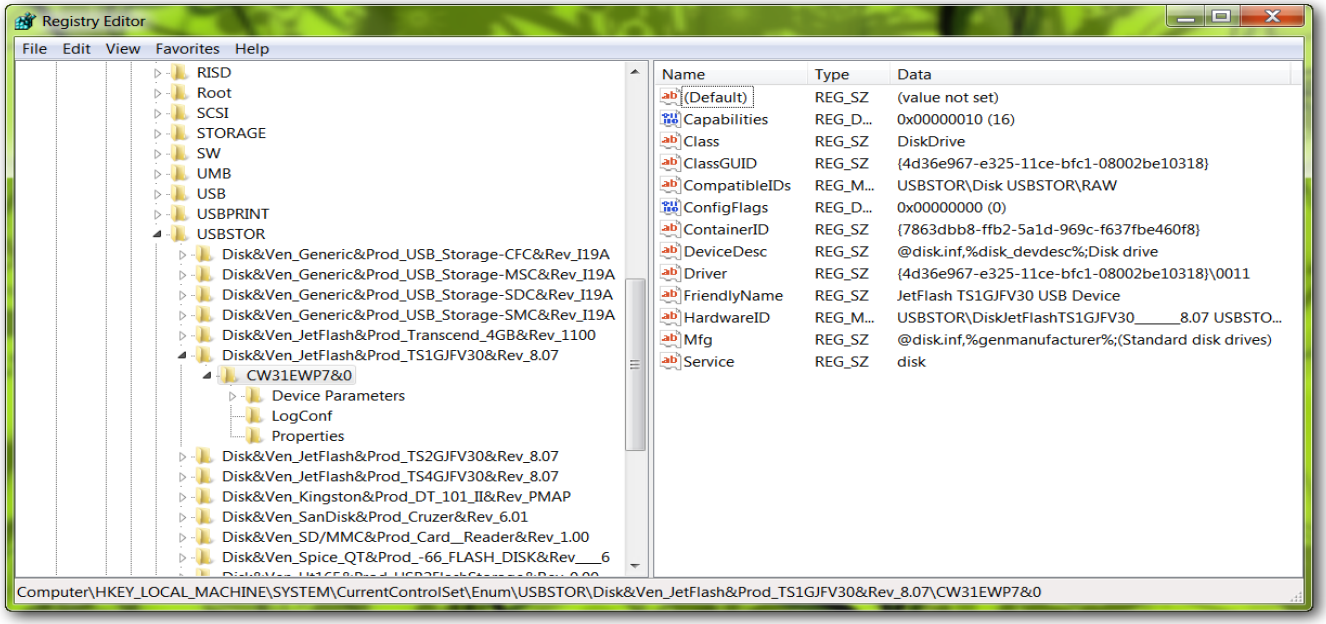

Figure 5: USB Device History

K. Information About Driver:

HKEY LOCAL MACHINE\ System\ControlSet\Enum

The Enum subkey contains information about every driver, device, or service that might potentially be attached to the machine. For example, Enum contains entries for the ATAPI driver even on machines with no ATAPI interface. These keys are used by the system to map devices and services with their drivers and configuration data. Besides, Enum stores information about the external storage devices such as a CD/DVD-ROM drive, a USB drive, or an external hard drive.

As the price of storage devices becomes cheaper, it is a general tendency that most people use high capacity external storage media. If the forensic analyst realize in the initial analyzing process that the suspect have used external storages, the opportunity that the suspect throw away or destroy them will decreases.

V. PROPOSED SYSTEM

Complex structure of windows 7 registry and lack of single proper documentation produce deterrence of forensics investigator towards windows registry analysis. But registry is a gold mine for evidence collection that inspired us to design a tool for registry analysis. The design of tool is shown in Fig 6.

Tool will collect information from live system as well as can be used to get information from hive file images which are captured for offline analysis by carving the internal structure of registry.

Reganalyzer will take input as list of plug-ins and image of hive files (in case of offline analysis) and process them to produce a report consisting of extracted data from registry as described in the plugins.

RegAnalyzer will analyze registry on windows system and collect information from the registry as per the selected plug-in in the analysis. Some of the information is given below:

a. Basic information about windows user like owner name, its environment settings.
b. Details of Operating System such as version, Service Pack installed, installation date
c. Last Write Time of registry key for creating timeline of events
d. Information about USB devices connected to system
e. Internet History of user activities
f. Analyze registry information of most popular applications installed on system like uTorrent, MS Office, Firefox, etc

Following are some useful features that will help forensic analyst are:

a. RegAnalyzer will record time when the registry was modified and also calculate hash of registry keys for maintaining integrity throughout the analysis.
b. RegAnalyzer will log the event perform by it.
c. RegAnalyzer tool will have option to generate the report that is used for documenting the analysis.
d. RegAnalyzer will be modular and can be extended by adding new plug-in.
e. RegAnalyzer tool will also provide easy GUI to create user plug-ins.

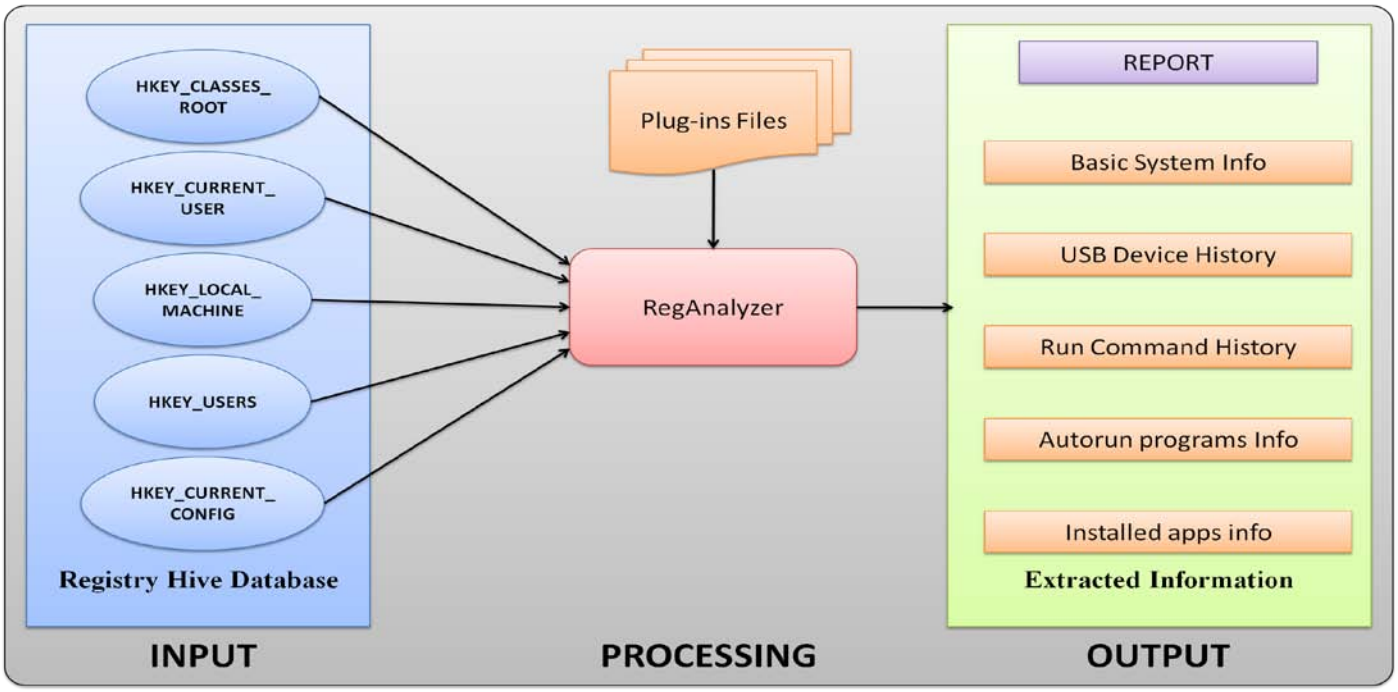

Figure 6: Architecture of RegAnalyzer

Algorithm Used in RegAnalyzer:

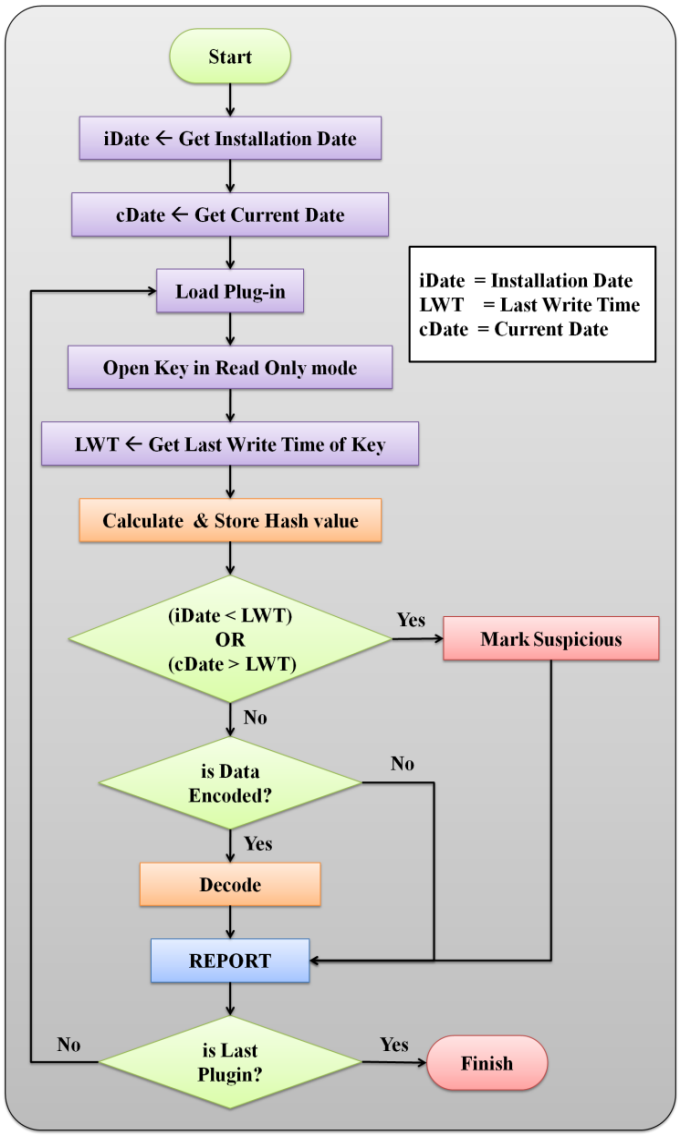

Figure 7: RegAnalyzer's Flowchart for processing registry

Description of RegAnalyzer's algorithm is given below:

INPUT: Tool will take list of plug-ins and windows registry as input.

PROCESSING: Following steps will be followed to process Registry Keys as shown in Fig. 7:

Step1: Store system installation date in iDate constant. This date will be calculated based on File Creation Time of randomly chosen system files, value of Registry key *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion/InstallDate* and Last Write Time of this key to verify integrity. iDate will act as lower limit for LastWrite Time of Registry key.

Step2: Get the current system date & time and store it in variable cDate. This will act as upper limit to the LastWriteTime of Registry Keys.

Step3: Load the first selected plug-in. Plug-in will have the information about the registry entries which should be processed for collecting evidences.

Step4: Open the Registry Key mentioned in the plug-in in ReadOnly Mode. Because of this no Registry Key or its values can be altered accidently. This is important to maintain integrity of evidence under consideration

Step5: Get the LastWriteTime of selected Registry Key. This can be done using the API provided by programming languages.

Step6: Calculate the hash value of Selected registry key which includes Registry Key name, its data type, its value and LastWriteTime. Store it in file to verify integrity whenever needed.

Step7: Check LastWrite Time of key is lying between iDate and cDate. If that is not the case then we can conclude that the key time may be externally modified by suspect. That Key will be marked suspicious in the report. This is simple check to detect malicious event.

Step8: Registry key values are not always stored in simple string or binary forms. Some values are stored in encoded forms for security. In this step the decoding of those values will be done.

Step9: All the events will be written in Report file. This file can be used for documentation purpose. It includes details of each registry key processed by plugins.

Step10: If processing of all selected plug-ins is completed the algorithm will stop otherwise it will continue from *Setp3.*

OUTPUT: Generated Report is the outpu of tool which has information about Registry Key, their decoded values, description of that Key related to forensic analysis.

VI. CONCLUSION

Windows 7 which is becoming the main operating system for home and business users. Most of the users are ignorant about the working of the system, therefore leaving footprints of their activity on the system and mainly in the registry. Analyzing that info gives forensic investigator initial information about the system environment and direction for further analysis.

Microsoft has provided very little information about the registry so it is difficult to refer large documents for registry analysis provided by other researchers. Thus, providing investigator a tool to supplement traditional registry analysis can give investigator an edge in forensic analysis by hiding unrelated information and highlighting the important information from registry.

The tool proposed in this paper will help forensic investigator to reduce the large amount investigation time spent on analysis of Windows Registry.

VII. REFERENCES

[1] Fauzan Mirza, Looking for Digital Evidence in Windows, Proc. International Symposium on Biometrics and Security Technologies, 2008, 1-7.

[2] Dr. Darren Hayes, Vijay Reddy, Shareq Qureshi, The Impact of Microsoft's Windows 7 on Computer Forensics Examinations, Proc. Applications and Technology Conference, Farmingdale, NY, 2010, 1-6.

[3] Muhammad Yasin, Muhammad Arif Wahla, Firdous Kausar, Analysis of Download Accelerator Plus (DAP) for Forensic Artefacts, Proc. Fifth International Conference on IT Security Incident Management and IT Forensics, 2009, 142-152.

[4] Ronald C. Dodge, Skype Fingerprint, Proc. 41st Hawaii International Conference on System Sciences, 2008.

[5] Brendan Dolan-Gavitt, Forensic analysis of the Windows registry in memory, Digital Investigation 5, 2008, S26-S32.

[6] Timothy D. Morgan, Recovering deleted data from the Windows registry, Digital Investigation 5, 2008, S33-S41.

[7] Paul McFedries, Microsoft Windows 7 Unleashed (United States of America, Library of Congress Cataloging-in-Publication Data, 2009) 225-244.

[8] http://msdn.microsoft.com/en-us/library/ms724871(v=VS.85).aspx

[9] Harlan Carvey, Windows Forensic Analysis DVD Toolkit 2E (United States of America, Syngress Publishing Inc., 2006) 157-259.