Forensic Investigation of User Activities on Windows7 & Ubuntu12 Operating System

Dinesh N. Patil
Veermata Jijabai Technological Institute,
Matunga, Mumbai(M..S.), India

B.B.Meshram
Veermata Jijabai Technological Institute,
Matunga, Mumbai(M..S.), India
bbmeshram@vjti.org.in

Abstract--- *Windows* operating system's registry contains information which are of potential evidential value or helpful in aiding forensic examiners to perform forensic analysis. Ubuntu operating system does not have registry like structure but its File System is evidential resource for the forensic examiner. This paper discusses the basics of Windows7 registry and its structure and Ubuntu12 File System. A comparative analysis of the Windows7 registry and Ubuntu12 file Systems entries for the various activities of the user related to Auto run Program, Recently Accessed documents , Application Settings, Malware Activity, Login & shutdown Activity, Network Accessed, Devices Connected to the System & their importance with respect to the digital forensic is performed.

Keywords - Windows registry, hive, key, forensic analysis, registry editor, Linux File System, digital forensic

I. Introduction

People with criminal mindset make use of the computer to perform various computer crimes such as hacking/cracking, network intrusion, computer viruses, industrial espionage etc. Computer users throughout the world are mainly using either Microsoft Windows or Linux operating systems. Therefore understanding the digital forensic importance of these operating systems has become essential to detect any malicious activity. Digital forensics deals with the collection and analysis of the digital information in an authentic, accurate way in order to identify the crime and the criminal.

In Windows operating systems, registry contains the configuration data that makes the operating system work; enables developers to organize configuration data in ways that are impossible using other mechanisms, such as .ini files; and is behind just about every feature that is available in Windows. The registry is introduced to replace most text-based configuration files used in Windows 3.x and MS-DOS, such as .ini files, autoexec.bat and config.sys. According to Microsoft Knowledge Base (KB) article [3], the Windows Registry is a "Central Hierarchal database" intended to store information that is necessary to configure the system for one or more users, applications, and hardware devices. Besides configuration information, the Windows Registry holds information regarding recently accessed files and considerable information about user activities.
Ubuntu operating systems does not have registry like structure but configuration information about the application, hardware devices and details of the various activity performed on the system by the users are recorded on various files maintained by the file system. Therefore a careful analysis of the Ubuntu file system is essential. A file system is the methods and data structures that an operating system uses to keep track of files on a disk or partition; that is, the way the files are organized on the disk. The file system refers to a partition or disk that is used to store the files or the type of the file system. On a UNIX system, everything is a file; if something is not a file, it is a process [8]. A Ubuntu system like UNIX makes no difference between a file and a directory, since a directory is just a file containing names of other files. Programs, services, texts, images, and so forth, are all files. Input and output devices, and generally all devices, are considered to be files, according to the system. In order to manage all these files, file system have been developed.

This paper is organized as follows: Section 2 includes the Literature Survey on the Windows7 Registry and Ubuntu12 File Systems and the related work done by the researchers. Section 3 presents the comparative forensic analysis of the various activities of the users recorded in the Windows7 registry & the Ubuntu12 file system and their application in determining the malicious intentions of the users. Section 4 concludes the results.

II. Literature Review

This section provides the forensic importance of the Windows 7 registry and the file system of Ubuntu12 for detecting any malicious activities of the users.

A. Related Work

Computer crimes are being done offline and online. Criminals steal the sensitive or personal data of the user from the Computer by login or by hacking the System. Criminals also can cause the system to get crashed so that it no longer works. In order to deal with such criminal activity & bring them to the justice 'Digital Forensics' techniques have been developed which involves Memory analysis and registry analysis, file system analysis in case of Windows, and Memory analysis, file system analysis to find the digital evidences of the criminal activity in case of Ubuntu12.The Microsoft Windows Operating System maintains the records of the activity on it in the form of registry and in Ubuntu its file system maintains the users activity.

Harlan Carvey [1] has provided the detailed information about the Windows registry structure and how it helps in getting the evidence of the user's activity. Jerry Honecutt [5] has provided the in-depth details of the Windows registry and how it helps in configuring the changes to the Computer system. Timothy D. Morgan [7] devised the technique to recover deleted data from the windows registry using the internal registry structure. The registry key can be recovered only if it has not been overwritten. Peter Hipson [4] provided detailed description of each and every key, sub key and their purpose in the Windows XP registry. Andrew Jones *et al*. [8] discussed some of the keys in the Windows 7 registry that are helpful to the forensic examiner. Once the relevant information's are obtained from these keys, it can reduce the effort required to do the investigation.
Therefore, extensive study of the Windows 7 registry to find out keys which can be of importance to the forensic examiner in investigating the criminal incidence is required.

Another widely used Operating System in the world today is Ubuntu, a Linux distribution. There is very little work done to know about, how the configuration information about device, application information and users activity, are maintained by the Ubuntu. Machteltt Garrells[9] has discussed about the Linux file system and the content of the directories .But the study of these with respect to the forensic importance have not been yet performed.

B. Windows7 Registry

By opening the Registry Editor (by typing regedit. in the run window), the Registry can be seen as one unified file system as in Figure 1.The left-hand pane, also known as the key pane contains an organized listing of what appear to be folders. The five most hierarchal folders are called root keys and begin with HKEY (An abbreviation for Handle to a Key). Although five root keys can be seen, only two of these are actually real i.e., HKEY_USERS (HKU) and HKEY_LOCAL_MACHINE (HKLM). The other three are shortcuts or aliases to branches within one of the two root keys HKU and HKLM. Physically, Windows organizes the registry in hives, each of which is in a binary file called a hive file. Only HKLM and HKU root keys consists of hives, the rest of the root keys are links to keys within these two root keys.

Each of these hives is composed of keys, which contain values and sub keys as shown in Figure 2. Values are the names of certain items within a key, which uniquely identify specific values pertaining to the operating system, or to applications that depend upon that value. Figure 2 shows Select key of the System hives consisting of value Last known Good configuration with data 0x0000002; which means the last known good configuration of the system is in controlset002; a forensic importance. The Keys are so similar to folders that they have the same naming rules. One or more keys can be nested within another key as long as the names are unique within each key. A key's name is limited to 512 ANSI or 256 Unicode characters, and any ASCII character in the name other than a backslash (\), asterisk (*), and question mark (?) can be used. In addition, Windows reserves all names that begin with a period for its own use. Each key contains one or more values. Each of these hives plays an important role in the function of the system.

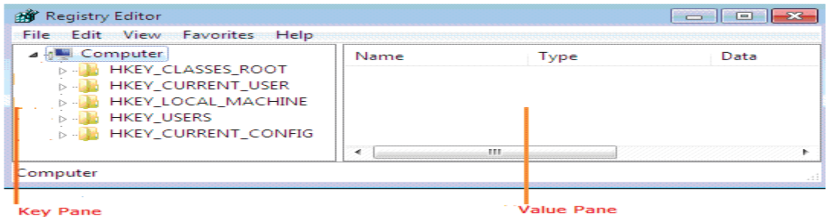


Figure 1. Window7 Registry Structure

The HKEY_CLASSES_ROOT hive contains configuration information relating to which application is used to open various files on the system. This hive is derived from the merging of HKEY_CURRENT_USER\Software\Classes (user-specific settings) and HKEY_LOCAL_MACHINE\Software\Classes (system wide settings).

The HKEY_CURRENT_USER is the actively loaded user profile for the currently logged-on user. This key is a link to HKEY_USERS\SID

The HKEY_LOCAL_MACHINE root key contains a vast array of configuration information for the system, including hardware settings and software settings. The HKEY_LOCAL_MACHINE hives are derived from the hive files which are present in the path

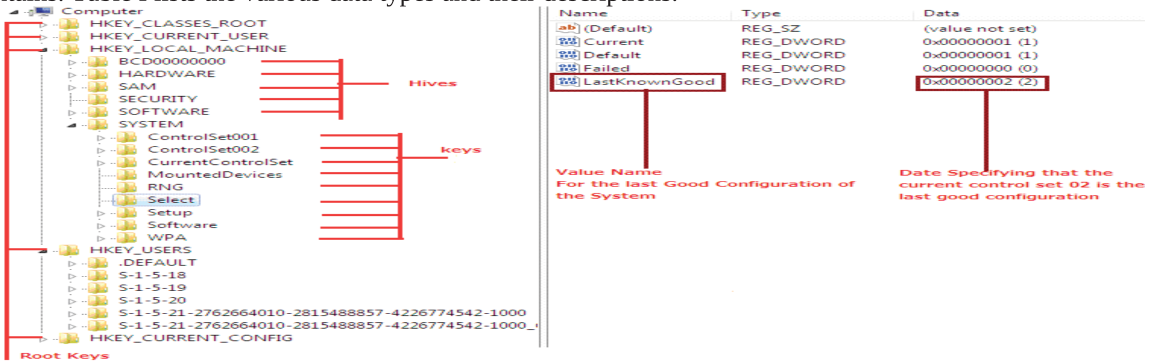
%SystemRoot%\System32\Config\

The HKEY_USERS root key contains all the actively loaded user profiles for that system. The HKEY_USERS hives are derived from the hive files ntuser.dat, UsrClass.dat and default.dat which are present in the paths respectively

%UserProfile%\NTUSER.DAT
UserProfile%\Local Settings\Application \Data \Microsoft \Windows\UsrClass.dat
%SystemRoot%\System32\Config\default

The HKEY_CURRENT_CONFIG hive contains the hardware profile the system uses at startup. This hive actually is a link to the HKLM\SYSTEM\CurrentControlSet\Hardware\Profiles \current

In addition to the different sections or hives, the Registry supports several different data types for the various values that it contains. Table I lists the various data types and their descriptions.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000002 (2)

Figure 2. Windows7 Registry with hive, key

C. *Ubuntu12 File System*

Linux uses more than one partition on the same disk. The reason why partitions have been used is for the security & robustness purpose. The breach of security on one partition does not affect the data on another partition.

There are two kinds of major partition on a Linux System [10]: Swap partition , Data partition

Swap partition is used for expansion of computer's physical memory, extra memory on hard disk, so that the Application programs are not required to be forcefully terminated due to lack of physical memory. Data partition consists of following different kind of pattern:

- A partition with all the data necessary to boot the system
- A partition with all configuration data
- A partition with user program and application
- One or more partitions for the user specific files

All partitions are attached to the system via a mount point. The mount point defines the place of a particular data set in the file system. Generally, all partitions are connected through the root partition which is indicated by slash (/). Various directories are created in the root partition.

Ubuntu12 uses the Linux file system which is usually considered as a tree structure as depicted in figure 3. Directories below the root directory are referred to as sub directory. The various sub directories of the root directory and its content are described as follows:

- /bin: stores common programs, shared by the system, the system administrator and the users
- /etc: stores system wide configuration files
- /usr: It consist of most program files
- /home: Each user used to have subdirectory to store their personal files
- /Media: Removable media will be mounted on this directory
- /var/log: Contains log files maintained by many applications

Every directory in Ubuntu12 has a path that starts in the root directory ('/') and ends in the directory's own name

Table -1 Registry Data Types

	Type	Value	Forensic Importance
1	REG_SZ	A String value	A fixed length text sting, understandable
2	REG_EXPAND_SZ	An expandable string data that can contain environment variable	This data type include variables that are resolved when a program or services uses the data
3	REG_BINARY	Binary data	Most Hardware Component Information is stored in this format
4	REG_DWORD_LITTLE_ENDIAN	A DWORD value , a 32-bit unsigned integer	Many parameters for device drivers and services are of this type
5	REG_DWORD_BIG_ENDIAN	A DWORD value , a 32-bit unsigned integer	Many parameters for device drivers and services are of this type
6	REG_MULTI_SZ	A multi string value ,which is an array of unique strings	Values that contain list or multiple values in a form that people can read
7	REG_RESOURCE_LIST	Resource List	Used for devices of the system
8	REG_FULL_RESOURCE_DESCRIPTOR	Resource Descriptor	Description of the Resource

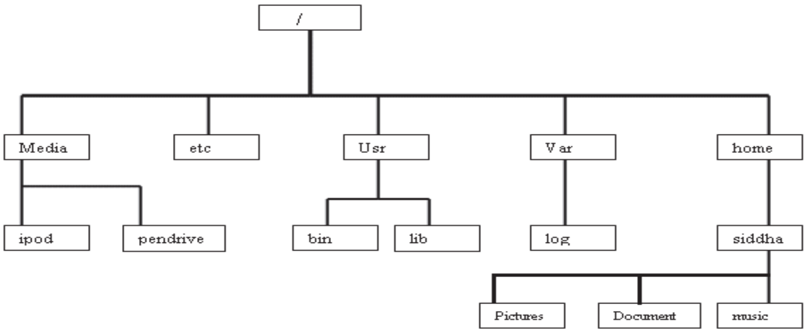


Figure 3. Ubuntu12 File System structure

III. FORENSIC ANALYSIS OF WINDOWS7 AND UBUNTU12

This section performs the comparative forensic analysis of the various activities of the users recorded in the Windows7 registry & the Ubuntu12 file system. The forensic analysis leads in determining the malicious code present in the system, perpetrator of the crime, devices used in doing the crime, data accessed or corrupted, networks used.

The best place to start in Windows7 operating system is within the Registry hive files within the User Profile; there is the well-known NTUSER.dat hive file found in the root of the profile directory, and with more recent versions of Windows (Vista, Windows 7), the USRCLASS.dat hive is of greater usage.
There are several registry key which maintains the most recently used list these keys values when interpreted can be of use during analysis

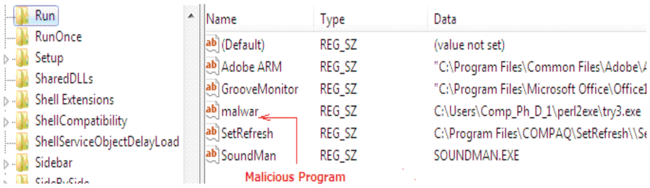
Similarly in Ubuntu12 Operating System , the information about the users activity are maintained in the file system The careful analysis of the file system will led to find helpful evidences of the users activity on the system.

A. Auto Run Program

Many programs are configured in such a way that when the Computer boot and start the operating system, they automatically start running such programs are called as Auto Run program. In Windows7, the Run key is used to maintain the information about such program. All of the available documentation at the Microsoft Web site indicates that when a user logs into a system, the contents of the Run key within the Software hive are run, and then the contents of the Run key within the user's hive are run; however, the entries within each key are run asynchronously, that is, in no particular order. Figure 4 shows the malicious code try3.exe included intentionally by the malicious user in the Run Key.The Run key within the user's hive is located in the following path:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

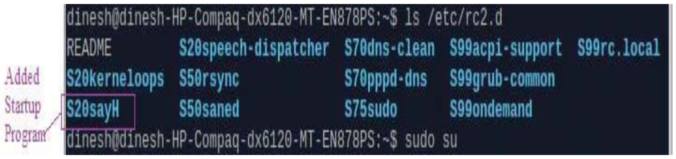
There are some malware which rely on this key for the persistence. Now, this key does not directly relate to user activity; rather, the contents of these key can help to understand the other applications may have been running when the user logged on to the system.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Adobe ARM	REG_SZ	"C:\Program Files\Common Files\Adobe\
GrooveMonitor	REG_SZ	"C:\Program Files\Microsoft Office\Office1
malwar	REG_SZ	C:\Users\Comp_Ph_D_1\perl2exe\try3.exe
SetRefresh	REG_SZ	C:\Program Files\COMPAQ\SetRefresh\\Se
SoundMan	REG_SZ	SOUNDMAN.EXE

Figure 4. Run Key with Malicious code path

The purpose of identifying this key and their contents, particularly during incident response or digital forensics analysis, would be to understand if the user purposely took specific actions that led to the issue (unusual or suspicious traffic observed on the network, and so on), or if the identified issue was due to some other processes at work, whether they are legitimate applications or malware. Understanding and examining malware persistence mechanisms (particularly those within the Registry) can also assist in addressing the "Trojan Defense,"



```
dinesh@dinesh-HP-Compaq-dx6120-MT-EN878PS:~$ ls /etc/rc2.d
README        S20speech-dispatcher  S70dns-clean  S99acpi-support  S99rc.local
S20kerneloops  S50rsync             S70pppd-dns   S99grub-common
S20sayH       S50saned              S75sudo       S99ondemand
dinesh@dinesh-HP-Compaq-dx6120-MT-EN878PS:~$ sudo su
```

Figure 5 rc2.d Directory files

In case of Ubuntu12 , the information about the programs which are to be executed when system booted is available in the file stored /etc/rc.d directory. The malicious user might gain an access to the Ubuntu system & will add files in rc.d directory such as 'sayH' in figure 5 to execute its malicious script. So whenever the Ubuntu12 System will boot up the malicious script will automatically run. The forensic examiner will have to look into those files to identify if any file contains malicious code which may be causing unauthorized activity on the system.

B. Recently Accessed Documents

In order to perform malicious activities users may access certain files on the Computer using Application Program. By knowing the Information about the documents that the user has recently accessed, the forensic examiner can know about, in which documents the user has interest. In addition to RecentDocs key, which provides the information about the documents recently accessed by the user, the History value also helps in knowing the recently accessed documents by the user. The RecentDocs key of Windows 7 is available in the following path:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\

The History value is available in the following path:

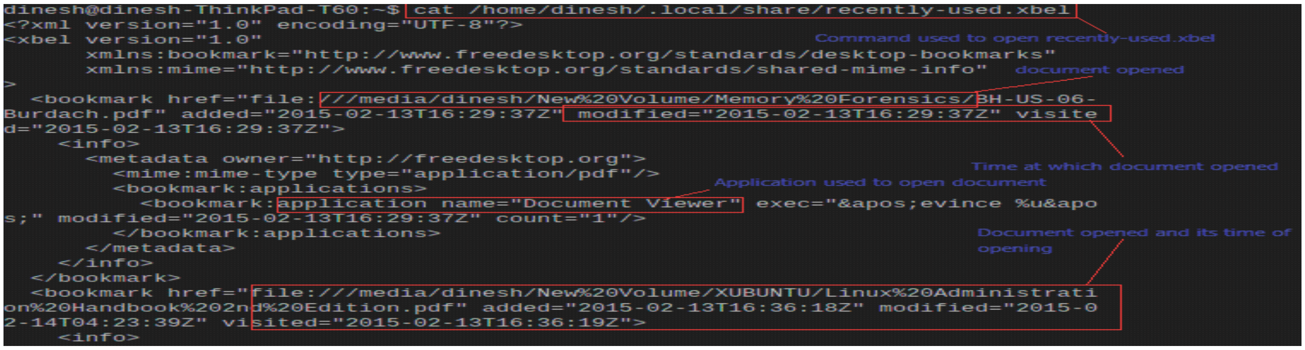
\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserShellFolders

The History value's data which is a path. It provides us the information about the files which have been recently accessed by the user. The History value has following data:

%USERPROFILE%\AppData\Local\Microsoft\Windows\History

In Ubuntu12, the files which have been recently accessed are noted in the file 'recently-used.xbel'. This file is available in the local/share/ directory. The 'cat' command can be used to read the contents of the recently-used.xbel file as shown in figure 6. Recently-used.xbel file provides the detailed information about the files which have been accessed by the user, the application used to access those documents and the timing of accessing & modifying these documents.

The recently accessed document information helps in understanding the files which may have been read, modified by the user.



```
dinesh@dinesh-ThinkPad-T60:~$ cat /home/dinesh/.local/share/recently-used.xbel
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
      xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
      xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info"
>
  <bookmark href="file:///media/dinesh/New%20Volume/Memory%20Forensics/BH-US-06-
Burdach.pdf" added="2015-02-13T16:29:37Z" modified="2015-02-13T16:29:37Z" visite
d="2015-02-13T16:29:37Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="application/pdf"/>
        <bookmark:applications>
          <bookmark:application name="Document Viewer" exec="&apos;evince %u&apo
s;" modified="2015-02-13T16:29:37Z" count="1"/>
        </bookmark:applications>
      </metadata>
    </info>
  </bookmark>
  <bookmark href="file:///media/dinesh/New%20Volume/XUBUNTU/Linux%20Administrati
on%20Handbook%202nd%20Edition.pdf" added="2015-02-13T16:36:18Z" modified="2015-0
2-14T04:23:39Z" visited="2015-02-13T16:36:19Z">
    <info>
```

Command used to open recently-used.xbel
document opened
Time at which document opened
Application used to open document
Document opened and its time of opening

Figure 6. recently-used.xbel location

C. *Application Settings*

One of the really useful aspects of the Windows operating systems is that when a user opens an application and modifies the location and size of the application window, those settings are saved so that the next time the user opens the application; the window is right back to where the user left it. This is addressed in part in MS KB article 813711 [2]. The Application's User-specific configuration and settings information is maintained in the following path:

HKEY_CURRENT_USER\Software\

Whereas the Machine-specific settings are stored in the following path:

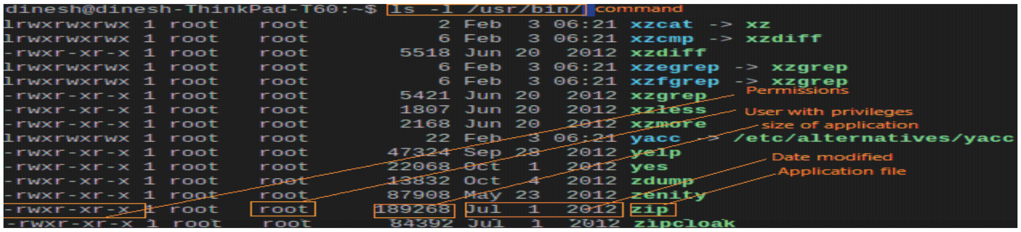
HKEY_LOCAL_MACHINE\Software\

In addition to this many application also adds their settings to the Uninstall key available in the following path:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\

Using these Keys, it is possible know the application programs installed by the user in order to access certain files or damage the system. After doing malicious activity using application, user may uninstall application. But the traces of the application may be left in one of these keys. If not there, then certainly some traces will remain on the hard disk

In Ubuntu12, the configuration information about the application is stored in the /usr/bin directory and the library required for these applications is available in the /usr/lib directory. The list of the application installed can be obtained by the command ls –l /usr/bin/ as shown in figure 7 .The directory /usr/share/ application also provides the graphical view of the application installed.



```
dinesh@dinesh-ThinkPad-T60:~$ ls -l /usr/bin/
lrwxrwxrwx 1 root    root          2 Feb  3 06:21 xzcat -> xz
lrwxrwxrwx 1 root    root          6 Feb  3 06:21 xzcmp -> xzdiff
-rwxr-xr-x 1 root    root       5518 Jun 20  2012 xzdiff
lrwxrwxrwx 1 root    root          6 Feb  3 06:21 xzegrep -> xzgrep
lrwxrwxrwx 1 root    root          6 Feb  3 06:21 xzfgrep -> xzgrep
-rwxr-xr-x 1 root    root       5421 Jun 20  2012 xzgrep
-rwxr-xr-x 1 root    root       1807 Jun 20  2012 xzless
-rwxr-xr-x 1 root    root       2168 Jun 20  2012 xzmore
lrwxrwxrwx 1 root    root         22 Feb  3 06:21 yacc -> /etc/alternatives/yacc
-rwxr-xr-x 1 root    root      47324 Sep 28  2012 yelp
-rwxr-xr-x 1 root    root      22068 Oct  1  2012 yes
-rwxr-xr-x 1 root    root      13832 Oct  4  2012 zdump
-rwxr-xr-x 1 root    root      87908 May 23  2012 zenity
-rwxr-xr-x 1 root    root     189268 Jul  1  2012 zip
-rwxr-xr-x 1 root    root      84392 Jul  1  2012 zipcloak
```

Figure 7. Application list of Ubuntu

Using the information available in the bin directory, analyst can provide the historic view of the application configuration that the user has installed onto the system, date on which a particular application was modified, permissions granted to the user, size of the application etc.

D. Malware activity

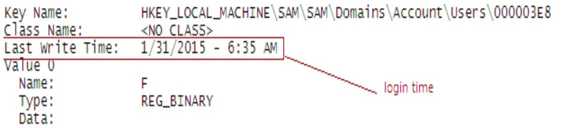
The MuiCache registry key can be useful for the analysis of malware on the Windows7, the path to the MuiCache key is:

\HKEY_CURRENT_USER\Software\Classses\Local\settings \MuiCache\31\52C64B7E\
When a malware run, the operating system creates a value in the MuiCache, as a result of how the malware was being launched within the testing environment. It is essential to look into MuiCache to find out traces of Malware.
To remain running after reboots, malware is usually re-launched using some persistence mechanism available in the various startup methods on a Ubuntu system, including services, drivers, scheduled tasks, and other startup locations. There are several configurations files that Ubuntu12 uses to automatically launch an executable when a user logs into the system that may contain traces of malware programs. Malware often embed itself as a new, unauthorized service.
Ubuntu12 has number of scripts that are used to start the service as the computer boots. The startup scripts are stored in /etc/init.d. Malware program may embed itself in /etc/init.d directory to run as a service and harm the system. Therefore the forensic examiner will have to look into those files to check for malware.

E. Login and shutdown Activity

In case of Windows7 Last Shutdown time of the System can be accessed using the following path:

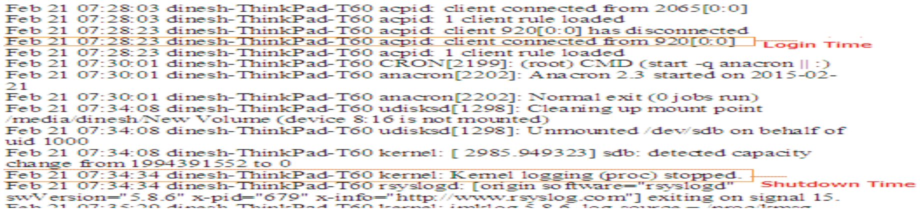
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Windows
And the time at which the user has first performed the login to the system can be accessed using the following path:
HKEY_LOCAL_MACHINE\SAM\Domains\Account\Users



```
Key Name:          HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000003E8
Class Name:        <NO CLASS>
Last Write Time:   1/31/2015 - 6:35 AM
Value 0
  Name:            F
  Type:            REG_BINARY
  Data:
```

Figure 8. A Users Account Key exported as .txt file

The login time is obtained by exporting the particular user account and saving it as .txt file as shown in figure 8
Using the login time and shutdown time, the forensic examiner can determine the actual duration of the use of the system for doing the crime.
In Ubuntu12 the login time and the logout time can be accessed by using the 'last' command at the terminal. Syslog file in the /var/log maintains the login and shutdown time as shown in figure 9



```
Feb 21 07:28:03 dinesh-ThinkPad-T60 acpid: client connected from 2065[0:0]
Feb 21 07:28:03 dinesh-ThinkPad-T60 acpid: 1 client rule loaded
Feb 21 07:28:23 dinesh-ThinkPad-T60 acpid: client 920[0:0] has disconnected
Feb 21 07:28:23 dinesh-ThinkPad-T60 acpid: client connected from 920[0:0]
Feb 21 07:28:23 dinesh-ThinkPad-T60 acpid: 1 client rule loaded
Feb 21 07:30:01 dinesh-ThinkPad-T60 CRON[2199]: (root) CMD (start -q anacron || :)
Feb 21 07:30:01 dinesh-ThinkPad-T60 anacron[2202]: Anacron 2.3 started on 2015-02-
21
Feb 21 07:30:01 dinesh-ThinkPad-T60 anacron[2202]: Normal exit (0 jobs run)
Feb 21 07:34:08 dinesh-ThinkPad-T60 udisksd[1298]: Cleaning up mount point
/media/dinesh/New Volume (device 8:16 is not mounted)
Feb 21 07:34:08 dinesh-ThinkPad-T60 udisksd[1298]: Unmounted /dev/sdb on behalf of
uid 1000
Feb 21 07:34:08 dinesh-ThinkPad-T60 kernel: [ 2985.949323] sdb: detected capacity
change from 1994391552 to 0
Feb 21 07:34:34 dinesh-ThinkPad-T60 kernel: Kernel logging (proc) stopped.
Feb 21 07:34:34 dinesh-ThinkPad-T60 rsyslogd: [origin software="rsyslogd"
swVersion="5.8.6" x-pid="679" x-info="http://www.rsyslog.com"] exiting on signal 15.
```

Figure 9. Syslog file view

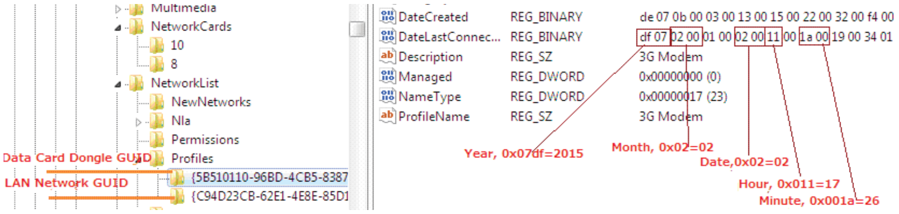
The analyst can predict the criminal, if the crime had happened during the duration of the use of the system by the user.

F. Networks Accessed/Connected

In order to perform data transfer to the remote computer, user will be required to get connected to the network, the type of network used by the user whether it is wireless or wired network is available in the Profile sub key of the Network List key ,available in the following path:

\HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles\
The Date & time at which the user has last connected to the particular network can be known from the value DateLastConnected as shown in figure 10.

Ubuntu12 maintains the list of networks connected to the system in /etc/NetworkManager/system-connections. In addition to this it is possible to know the active network connections which are being used in the system using the command “sudo netstat –tupn “

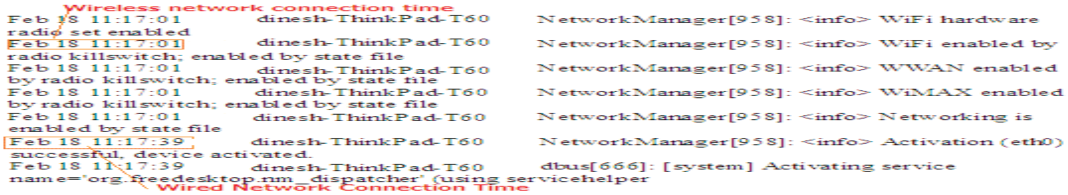


```
Multimedia
NetworkCards
    10
    8
NetworkList
    NewNetworks
    Nla
    Permissions
    Profiles
        {5B510110-96BD-4CB5-8387
        {C94D23CB-62E1-4E8E-85D1
```

```
DateCreated       REG_BINARY   de 07 0b 00 03 00 13 00 15 00 22 00 32 00 f4 00
DateLastConnec... REG_BINARY   df 07 02 00 01 00 02 00 11 00 1a 00 19 00 34 01
Description       REG_SZ       3G Modem
Managed           REG_DWORD    0x00000000 (0)
NameType          REG_DWORD    0x00000017 (23)
ProfileName       REG_SZ       3G Modem
```

Figure 10. Network List

Syslog file in /var/log provides the date and time at which a particular network connection was established as shown in figure 11. Network information enables the forensic examiner to know about the type of network used in order to do malicious activity



```
Feb 18 11:17:01        dinesh-ThinkPad-T60        NetworkManager[958]: <info> WiFi hardware
radio set enabled
Feb 18 11:17:01        dinesh-ThinkPad-T60        NetworkManager[958]: <info> WiFi enabled by
radio killswitch; enabled by state file
Feb 18 11:17:01        dinesh-ThinkPad-T60        NetworkManager[958]: <info> WWAN enabled
by radio killswitch; enabled by state file
Feb 18 11:17:01        dinesh-ThinkPad-T60        NetworkManager[958]: <info> WiMAX enabled
by radio killswitch; enabled by state file
Feb 18 11:17:01        dinesh-ThinkPad-T60        NetworkManager[958]: <info> Networking is
enabled by state file
Feb 18 11:17:39        dinesh-ThinkPad-T60        NetworkManager[958]: <info> Activation (eth0)
successful, device activated.
Feb 18 11:17:39        dinesh-ThinkPad-T60        dbus[666]: [system] Activating service
name='org.freedesktop.nm_dispatcher' (using servicehelper
```

Wireless network connection time
Wired Network Connection Time

Figure 11 Current Network Connection

G. Devices Connected to the System

The malicious user attaches hardware devices to perform various tasks like printing the documents, copying the files. The List of the Hardware devices including the processor attached to the System can be known from the HARDWARE hive file in the Windows7 registry as shown in figure 16 .The processor information can be found in the following path:

\HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\

The USB device attached to the Computer, its entry is made in the following registry key of the Windows7:

\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\

The time at which a particular device was attached to the Computer can be obtained from the USB key:

\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\
Whereas the rest of the hardware devices information can be known from the path:

\HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\

In Ubuntu12 “lshw” command provides the list of hardware devices attached to the system. Also the /dev directory in the file system provides the information about the hardware attached to the system. The syslog file also maintains the details of the devices which have been detected as shown . The date and timing at which the device was connected along with device details are also recorded in the syslog

The device information provides the knowledge about the kind of devices and the time at which they were used in doing malicious activity.

IV.CONCLUSION

In Windows7 Operating System, a great deal of information is in the registry that will provide indications of not only what the user did but also when they did it. This can help demonstrate that on a system which kind of action performed by the user. An analyst can use all of this information to develop an understanding of and add context to other activity found on the system. Analysis of the registry can also assist in determining if the system was infected with malware, or if the user (or an intruder) was responsible for the observed activity.

Ubuntu does not have equivalent of the Windows like registry. Configuration is kept in (mostly) text files: The system configuration is in text files under /etc. The system state with configuration data, lives under /var. User configuration and state lives in “dot files”, i.e., files and directories whose name begins with a .(dot) in your home directory. The syslog file in the /var/log records each and every activity from the boot of the system to the shutdown.

Ubuntu12 file system; provides help to the forensic examiner in doing some real investigation of the user activity and tracking malicious activity

REFERENCES

[1] Harlan Carvey, Windows Forensics Analysis, Syngress publication , 2011

[2] Microsoft Support.” My view settings or customization for a folder are lost or incorrect” http://support.microsoft.com/kb/813711, 15 July 2009

[3] Microsoft Support, Windows registry information for Advanced users, http://support.microsoft.com/kb/256986,Dec., 2013.

[4] Peter Hipson, Mastering Windows XP Registry, SYBEX Inc.,2002

[5] Jerry HoneyCutt , Microsoft Windows Registry Guide, Second Edition, Microsoft Press, 2005

[6] Carvey, Harlan. "The Windows Registry as a Forensic resource." Digital Investigation: The International Journal of Digital Forensics & Incident Response 2(2005): 201-05,2005

[7] Timothy D. Morgan, ”Recovering Deleted data from the Windows Registry”, digital Investigation 5(2008) S33-S-41,2008

[8] Alghafli, K.A & Jones, A & Martin T.A. (2010) .Forensic Analysis of the Windows7 Registry. 8th Australian digital Forensic Conference,2010

[9] Machtelt Garrels,Introduction to Linux: A hands on Guide, 2004

[10] Binh Nguyen, Linux File System Hierarchy, version 0.65,2004

[11] Harlan Carvey, Digital Forensics with Open Source tools, Syngress,2011

[12] Ministry of Law, Justice and Company Affairs, Government of India, Information Technology Act 2000,9th June 2000

[13] M. Keeney, E. Kowalski, D. Cappelli, A. Moore, T, himeall, S.Rodgers, “Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors”, Jan 2005

[14] E. Shaw, K. Ruby, and J. Post, “Insider Threats to Critical Information Systems: Typology of Perpetrators, Security Vulnerabilities, Recommendations”,. ASD-C3I – OIO - Contract # 98-G-7900, Task Letter Number 001:Insider Threat Profile Aug 31, 1999