Digital Forensic Identification, Collection, Examination and Decoding of Windows Registry Keys for Discovering User Activities Patterns

Abhijeet Ramani, Somesh Kumar Dewangan

Department of Computer Science and Engineering, CSVTU University, Bhilai Chhattisgarh
Disha Institute of Management and Technology, Raipur, Chhattisgarh, India

***Abstract*—The Key study in this paper is to begin the investigation process with the initial forensic analysis in the segments of the storage media which would definitely contain the digital forensic evidences. These Storage media Locations is referred as the Windows registry. Identifying the forensic evidence from windows registry may take less time than required in the case of all locations of a storage media. Our main focus in this research will be to study the registry structure of Windows 7 and identify the useful information within the registry keys of windows 7 that may be extremely useful to carry out any task of digital forensic analysis. The main aim is to describe the importance of the study on computer & digital forensics. The Idea behind the research is to implement a forensic tool which will be very useful in extracting the digital evidences and present them in usable form to a forensic investigator. The work includes identifying various events registry keys value such as machine last shut down time along with machine name, List of all the wireless networks that the computer has connected to; List of the most recently used files or applications, List of all the USB devices that have been attached to the computer and many more. This work aims to point out the importance of windows forensic analysis to extract and identify the hidden information which shall act as an evidence tool to track and gather the user activities pattern. All Research was conducted in a Windows 7 Environment.**

***Keywords*—Windows Registry, Windows 7 Forensic Analysis, Windows Registry Structure, Analysing Registry Key, Digital Forensic Identification, Forensic data Collection, Examination of Windows Registry, Decoding of Windows Registry Keys, Discovering User Activities Patterns, Computer Forensic Investigation Tool.**

I. INTRODUCTION

Today in the Techno World there is an innovative evolution in technologies that have became part of our life. Things are made available just at a click, from any available target communicating device. Information can be accessed with an ease, no matter at what place you are, what the time is or what the device you are using. Actually, the technology has revolutionized the working culture. The professionals and users have adapted the information browsing process through the available innovative technology to maintain and upgrade their job profile.

Illegal activities and crimes have also increased with the enhancement in technology. Many Enterprises and organizations are suffering from these computer crimes and the criminals that perpetrate them have a wide variety of motivations. Criminological activity includes Exploitation of Wireless Network, Denial of Service attack, Financial fraud, Password sniffing, Zombies within organization, information sniffing from computer and copying them to flash drives, Malware infection, phishing and many more. Since crimes have moved into the computing environment, a new field in forensic investigations has appeared which is called Computer Forensics, but this is now more commonly referred to as digital forensics. There are many ways of computer forensic investigation. The way used in this research has been implemented on forensic analysis in windows 7 registry.

In this paper, the basic aim is to study about Windows 7 Registry and implement a forensic tool to carefully investigate the windows 7 registry and track down the user actions and events whose result will be very useful for digital forensic examination in various crime scenes. In the coming sections we will see the ways to analyze windows registry manually and find out the footprints of user activities. The result will answer out the importance of digital forensic investigation by presenting the role played by windows registry. The manual process of analyzing windows registry is very tedious as the registry values are encoded with hexadecimal number system. The tool was designed to ease with the investigating process by decoding the registry key values and presenting them in normal readable form to forensic investigator.

In brief, windows registry analysis can run across a variety of processes & activities, for extracting various key and transforming it into a meaningful evidence to trace the user, system, application & network timeline using forensic study.

In this paper we have discussed about the forensic analysis on Windows 7 Registry. We begin by stating the work done by various researchers in section II, and will be discussing about the revolutionized change that has been there in the field of forensic investigations. In the section III we will be discussing the basics of Windows Registry and will go through the important locations in the hierarchy of the windows registry to do the forensic investigation process. After this, the discussion will be on result obtained followed by conclusion & future scope.

II. Related Work

Over the past several years, with computer crimes on the rise, 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. During the last fifteen years or so, computers have revolutionized the work place. Information and critical data needed by the workers are stored into computers. The operating system allows imposing various security techniques and group policies to maintain the CIA (Confidentiality, Integrity & Authenticity) security principles. However, regardless of the policies and rules it's not easy to persist with the CIA principles. Researchers are coming with new ideas to protect the critical data. One such technique "Forensic Analysis of the Windows Registry" has emerged and is becoming a burning topic in the field of network and information security.

An Ample of information was analyzed by Carvey [2] on applying digital forensic analysis of the windows registry. Carvey has focused on the windows registry structure and suggested the methods- Live analysis and forensic analysis.

Farmer [3] has introduced the Microsoft Windows Registry database and explained how critically important a registry information is to computer forensic experts. The papers discussed about the various types of Registry "footprints". Currently, there are many tools available to forensic examiners for extracting evidentiary information from the Registry. The tool used in this paper to analyze and navigate the registry is Registry Editor (regedit.exe). Registry Editor is free and available on any installation of Microsoft Windows XP with administrator privileges. The final conclusion, this report is by no means conclusive in terms of a Registry Examination. It presents some explanations and examples of what types of data can be found, how it can be found, and why it may be relevant to an examination.

Alghafli, K.A. & Jones, A. & Martin, T.A. [8] have illustrated the recovery of digital evidence of crimes from storage media in an increasingly time consuming process as the capacity of the storage media is in a state of constant growth. In this paper, the registry structure of Windows 7 is discussed briefly with several elements of information within the registry structure of Windows 7 that may be valuable to a forensic investigator. In this paper, the Registry structure of Windows 7 is discussed together with several elements of information within the Registry of Windows 7 that may be valuable to a forensic investigator. A tool was implemented to perform the simple forensics investigation on system, network and applications. There was not much work done on USB devices and no methodology was implemented to track the copying of data into the USB devices. No attempt was made to store the analyzed forensic data into the database due to which reporting was a tedious job. No concept of new case enrolment.

Jain, A. & Roy, T. [7] have conducted their research on Windows XP Registry structure. Registry is an important location in Windows system that contains foot_ prints of user activities and other configuration data, which may be valuable for forensic investigators in collecting potential evidences from the system. This work aims to point out the significance of Registry Analysis, and attempts to answer why it should be carried as a part of digital forensic investigation by demonstrating the role played by Registry in tracking data theft from system to USB external devices. But the research was not carried for the Windows 7 Registry Structure.

They have discussed, how by means of a careful investigation of the Registry files, data transfer to USB devices be identified and finally show how to proceed in a case involving data transfer from system to USB through Registry analysis. This paper has gathered and verified the existing knowledge about the registry hive files. They attempted to exhibit the importance of registry analysis by demonstrating how it can help an investigator to progress in a case of tracking data transfer from a system to a USB external device. This work is focused on the examination and generation of registry keys of Windows XP systems only, and can be extended further for the examination of registry files in Windows Vista, Windows 7 and other later versions.

Liming Cai, Jing Sha ,Wei Qian. [16] presented their research on Forensic Analysis of Physical Memory. In this paper they have firstly describe the importance of the study on forensics analysis of physical memory. Further they have introduced some tools and techniques commonly used in forensics analysis of physical memory. Lastly they have presented an example of forensic analysis to illustrate how to do physical memory forensics and analysis in a windows system by using existing tools. The key technology of forensics analysis of physical memory mainly includes two aspects: acquisition of physical memory and analysis of collected physical memory. That is to say, firstly how to obtain physical memory and generate physical memory image file; secondly how to find out important evidence through the analysis of physical memory image file. The final conclusion was as follows; Firstly, it is a lack of reliable and practical hardware device to access physical memory. Hardware based method to get the system's physical memory is an ideal solution as it almost doesn't affect system's physical memory. Secondly, although there are a lot of software tools for acquisition of system's physical memory, software tools will inevitably damage or even override the contents of physical memory. How to improve software tools to make minimize impact on physical memory is our next issue to research.

Haoyang Xie, Keyu Jiang, Xiaohong Yuan and Hongbiao Zeng [17] conducted a research on forensic analysis of windows registry against intrusion. This paper introduces the basics of Windows Registry, describes its structure and its keys and sub-keys that have forensic values. This paper also discusses how the Windows Registry forensic keys can be applied in intrusion detection. The final conclusion delivered was on Windows Registry Forensics. Keys and sub-keys that have forensic value are filtered from Windows Registry and organized. They could be considered as tools to investigate Windows Registry in real cases. As part of Windows Registry forensics, this paper discusses the applications of the forensic keys against intrusion. However, the keys filtered and organized in this paper are not all of the keys that have forensic values. Windows Registry is huge and the research on it continues. Even if we have known every key, sub-key, and value of Windows Registry, we still have to consider how to use them in real cases since the intrusion cases will not be the same every time.

Lih Wern Wong [18] carried the research on Forensic Analysis of the Windows Registry. This paper discusses the basics of Windows XP registry and its structure, data hiding techniques in registry, and analysis on potential Windows XP registry entries that are of forensic values.

An Essential Research was carried out on Retrieving Digital Evidence: Methods, Techniques and Issues by Yuri Gubanov[19]. This article describes the various types of digital forensic evidence available on users' PC and laptop computers, and discusses methods of retrieving such evidence.

The Research focuses strictly about digital evidence available on the PC or, more precisely, on the computer's hard drive and live memory dumps. This leaves the entire domain of mobile forensics aside, for a good reason: mobile forensics has its own techniques, approaches, methods and issues.

III. METHODOLOGY

A. Registry Definition

The Microsoft Computer Dictionary defines the registry as: "A *central hierarchical database* used in the Microsoft Windows family of Operating Systems to store information necessary to configure the system for one or more users, applications and hardware devices".

The registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can crate, property sheet settings for folders and application icons, what hardware exists on the system and the ports that are being used.

B. The Windows Registry Basics

Title Windows registry is a core of the operating system which determines the appearance and behaviour of windows. It is a central repository or a hierarchical database of configuration data for the Windows operating system. It has configuration data for all the installed software applications, device drivers, and policies pertaining to the system and the users. It controls the peripherals devices and how applications run. Every time an application runs in the Windows environment, the first thing it checks is the registry. Without accessing the registry no application can be started. In other words windows eventually fail if the registry fails. The analysis of Windows Registry involves not just viewing data within the registry but it is about extracting, interpreting, and understanding what that data means in its own context and in the context of a forensics investigation.

1) How to access the Windows Registry?

The Windows Registry is accessed and configured using the Registry Editor program, a free registry editing utility included with every version of Microsoft Windows. Registry Editor can be accessed by executing "regedit" from the Command Prompt or from the search or run box from the Start menu. Registry Editor is the face of the registry, and is the way to view and make changes to the registry, but it's not the registry itself. Technically, the registry is the collective name for various database files located within the Windows installation directory.

2) Windows Registry Structure:

A hive (Root Keys) in the Windows Registry is the name given to a major section of the registry that contains registry keys, registry sub keys, and registry values. All keys that are considered hives begin with HKEY and are at the top of the hierarchy in the registry. In Registry Editor, the hives are the set of registry keys that appear as folders on the left hand side of the screen when all other keys have been minimized.

Here is a list of the common registry hives in Windows:

i. HKEY_CLASSES_ROOT
ii. HKEY_CURRENT_USER
iii. HKEY_LOCAL_MACHINE
iv. HKEY_USERS
v. HKEY_CURRENT_CONFIG

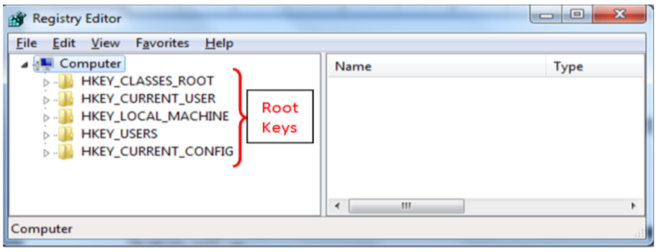


Fig. 1 Windows Registry root Keys

HKEY_CLASSES_ROOT-

It is a registry hive in the Windows Registry and contains file extension association information, as well as programmatic identifier (ProgID), Class ID (CLSID), and Interface ID (IID) data. In the simplest terms possible, the HKEY_CLASSES _ROOT registry hive contains the information necessary so Windows knows what to do when you ask it to do something, like view the contents of a drive, or open a certain type of file, etc. The list of registry keys under the HKEY_CLASSES_ROOT hive is very long. Here are some of the many file extension association keys you'll find under the HKEY_CLASSES_ROOT hive, most of which will be begin with a period:

HKEY_CLASSES_ROOT\.avi
HKEY_CLASSES_ROOT\.bmp
HKEY_CLASSES_ROOT\.exe
HKEY_CLASSES_ROOT\.html
HKEY_CLASSES_ROOT\.pdf
HKEY_CLASSES_ROOT\dllfile

Each of these registry keys stores information as to what Windows should do when you double-click on a file with that extension. For example, on my computer, when you double-click on a file by the name of *draft.rtf*, WordPad opens the file. The registry data that makes that happen is stored in the *HKEY_CLASSES_ROOT\.rtf* key. The HKEY_CLASSES_ROOT hive is actually combined data found in both the HKEY_LOCAL_MACHINE hive (*HKEY_LOCAL_MACHINE\Software\Classes*) and the HKEY_CURRENT_USER hive (*HKEY_CURRENT_USER \Software\Classes*). If a registry key resides in both locations, but conflicts in some way, the data found in *HKEY_CURRENT_USER\Software\Classes* is used in HKEY_ CLASSES_ ROOT. It can be accessed by clicking on the *HKEY_CLASSES_ROOT* hive on the left panel in Registry Editor.

HKEY_CURRENT_USER

It is one of a half-dozen or so registry hives, part of the Windows Registry. HKEY_CURRENT_USER contains configuration information for Windows and software specific to the currently logged in user. For example, various registry values in various registry keys located under the HKEY_CURRENT_USER hive control user-level settings like the printers installed, desktop wallpaper, display settings, keyboard layout, mapped network drives, and more. Many of the settings you configure within various applets in the Control Panel are stored in the HKEY_CURRENT_USER registry hive. Fig. 2 shows registry keys you might find under the HKEY_CURRENT_USER hive:

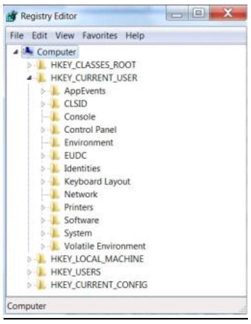


Fig. 2 HKEY_CURRENT_USERS Keys

Since the HKEY_CURRENT_USER hive is user specific, the keys and values contained in it will differ from user to user on the same computer. This is unlike most other registry hives which are global, meaning they retain the same information across all users in Windows. HKEY_CURRENT_USER can be accessed by clicking on the *HKEY_CURRENT_USER* hive on the left side of the Registry Editor program window. The HKEY_CURRENT_USER hive is actually just a pointer to the key located under the HKEY_USERS hive that's named the same as your security identifier. You can make changes in either location since they are one in the same.

HKEY_LOCAL_MACHINE

It is one of several registry hives in the Windows Registry. HKEY_LOCAL_MACHINE contains the majority of the configuration information for the software you have installed and for the Windows operating system itself. The HKEY_LOCAL_MACHINE hive also contains information about currently detected hardware. Fig. 3 shows registry keys you might find under the HKEY_LOCAL_MACHINE hive:

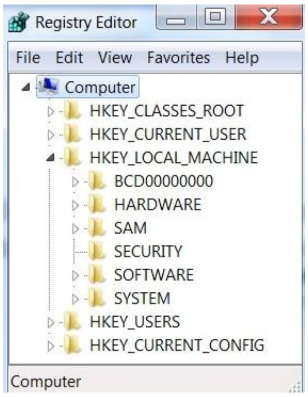


Fig. 3 HKEY_LOCAL_MACHINE Keys

HKEY_USERS

It is one of many registry hives in the Windows Registry. HKEY_USERS contains user-specific configuration information for all currently active users on the computer.

Each registry key located under the HKEY_USERS hive corresponds to a user on the system and is named with that user's security identifier, or SID. The registry keys and registry values located under each SID control settings specific to that user, like mapped drives, installed printers, desktop background, and much more. From Fig. 4, the details can be found out. The first four Keys are referred to as the System Accounts and will generally be the same from computer to computer. HKU\.DEFAULT contains global User information. HKU\S-1-5-18 pertains to the Local System Account. HKU\S-1-5-19 is used to run the local services and is the Local Service Account. HKU\S-1-5-20 is the Network Service Account which is used to run the network service(s). Other Sub keys are unique SIDs which are associated with individual Users and can be of considerable forensic importance. Their interpretation is as follows:

"S" identifies the string as an SID.

"1" is the version of the SID specification.

"5" is the identifier authority value.

"21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx" is the domain or local computer identifier. (Note: The numbering schema "xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx" will differ from computer to computer since it corresponds to individual, unique User accounts).

"1000" is the Relative ID (RID). Any Group or User not created by default will have an RID of 1000 or greater.

"1001_Classes" contains the per-User file associations and class registration.

A wealth of forensic information is contained in each SID. This includes the User's Name, the number of times the User logged onto the computer, the date and time of the last logon, the date and time the last password was changed, number of failed logons, and so on.

Here is an example (Fig. 4) of what you might find under the HKEY_USERS hive:

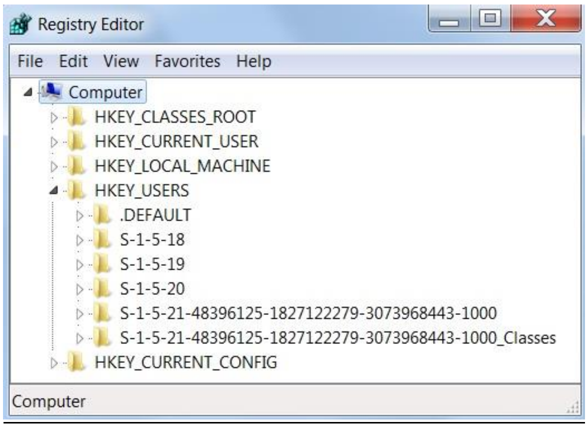


Fig. 4 HKEY_USERS Keys

HKEY_CURRENT_CONFIG

It is a registry hive, part of the Windows Registry, and stores information about the hardware profile currently being used. Actually, HKEY_CURRENT_CONFIG is simply a pointer to the *HKEY_LOCAL_MACHINE\SYSTEM \Current ControlSet\HardwareProfiles\Current*registry key, which in turn is just a pointer to the currently active hardware profile listed under the *HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\ CurrentControlSet\HardwareProfiles* key. So HKEY_ CURRENT_CONFIG really just exists so it's easy to view and modify this data, which you can do in any of the three locations since they are all the same. Here are the two registry keys shown in Fig.5. you will find under the HKEY_CURRENT_CONFIG hive:

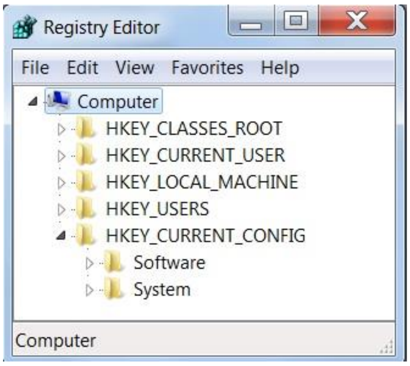


Fig. 5 HKEY_CURRENT_CONFIG Keys

3) Proposed System:

The Key study in this venture is to start the examination process with the beginning measurable investigation in the locations of the storage media which would without a doubt contain the traces of criminological confirmation evidences. These Storage media Location is referred as the Windows registry. Auditing the windows registry may take less time than needed on account of analysing complete storage media. The registry is the absolute building and running entirety of Microsoft Windows operating system. The windows registry contains the configuration information that makes the operating system to function properly; enables development platform programmers to work with these configuration settings in an accurate manner. Windows and each application that runs on Microsoft's operating system do literally nothing without counselling and consulting the registry first. When you double-click a file, Windows check with the registry configuration data to evaluate what to do with that clicked file. At the point when you plug-in a device, Windows allocates resources to the device focused around data in the registry and after that stores the device configuration data and settings in the registry. When you run an application, for example, Microsoft Office Word 2010, the application finds your preferences in the registry. Thus, it becomes extremely important for the forensic investigators to understand computer systems and be able to examine them carefully and effectively. From a technical standpoint, the main goal of computer forensics is to identify, collect, preserve, and analyse data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case. The objective is to implement a tool which identifies various registry keys value and fetch the data from them. The fetched data will be examine and decoded to collect the forensic information from the decoded data. This forensic information includes machine last shut down time along with machine name, List of all the wireless networks that the computer has connected to; List of the most recently used files or applications, List of all the USB devices that have been attached to the computer and much more important forensic functionality will be included. All efforts are just to trace the user activity behaviour.

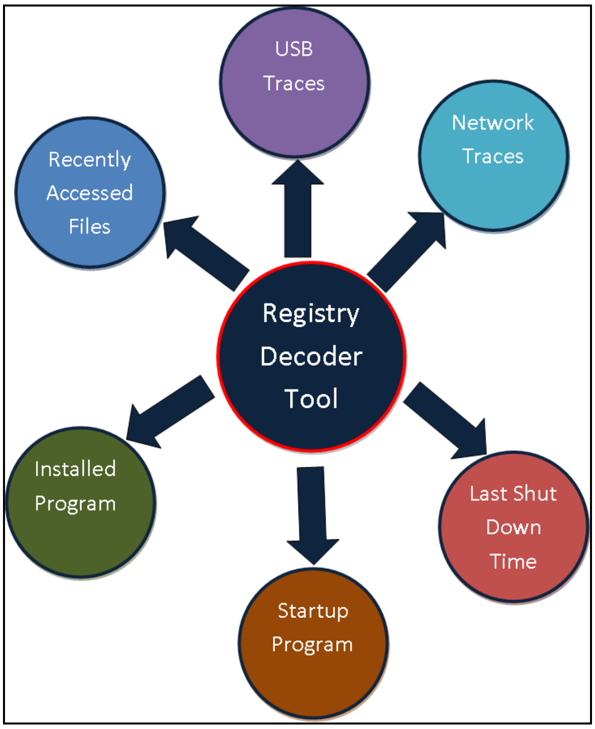


Fig. 6 The Objective: “Windows Registry Decoder Tool”

4) System Requirements

a) Supported Operating System
Windows 7, Windows Server 2003 R2 (32-Bit x86), Windows Server 2003 R2 x64 editions, Windows Server 2003 Service Pack 2, Windows Server 2008 R2, Windows Server 2008 Service Pack 2, Windows Vista Service Pack 2, Windows XP Service Pack 3.

b) Dot Net Framework 4.0

c) Microsoft Visual Studio 2010 Express Edition

5) Accessing the Registry with Visual Basic .NET

When programming in VB.NET, you can choose to access the registry by functions provided by registry classes of the .NET Framework which is present in Microsoft.Win32 namespace. The registry hosts information from the operating system as well as information from applications hosted on the machine. Working with the registry may compromise security. Therefore, you must closely scrutinize code that accesses the registry to ensure that it poses no threat to the security of the machine on which it will run. Registry entries contain two parts: the value name and the value. Entries are stored under keys and sub-keys in a system that is analogous to the file system, where files are stored in directories and subdirectories.

a) Namespace

The namespace used in visual basic using .NET framework to obtain access to the manipulation tools of the registry is “Microsoft.Win32” Access to the elements of registry control can also be obtained using this namespace. Following are the two main classes included in the namespace. The Microsoft.Win32 namespaces provide types that handle events raised by the operating system, that manipulate the system registry, and that represent file and operating system handles.
The Microsoft.Win32 namespace provides two types of classes: those that handle events raised by the operating system and those that manipulate the system registry.
.NET Framework Library provides two classes - Registry and RegistryKey to work with the registry. These classes are defined in Microsoft.Win32 namespace. So before using these classes, you need to add reference to this namespace.

b) Registry Class

Provides RegistryKey objects that represent the root keys in the Windows registry, and static methods to access key/value pairs. The Registry class is used to represent the main seven sub-nodes of the registry that are to be accessed and manipulated. In the Visual Studio.NET and the namespace provides seven nodes.

c) RegistryKeyClass

This Class represents a key-level node in the Windows registry. This class is a registry encapsulation. The most important class used for manipulating the registry in Visual Basic is the RegistryKey Class. Several methods are available in the class which either produce data or delete the data.

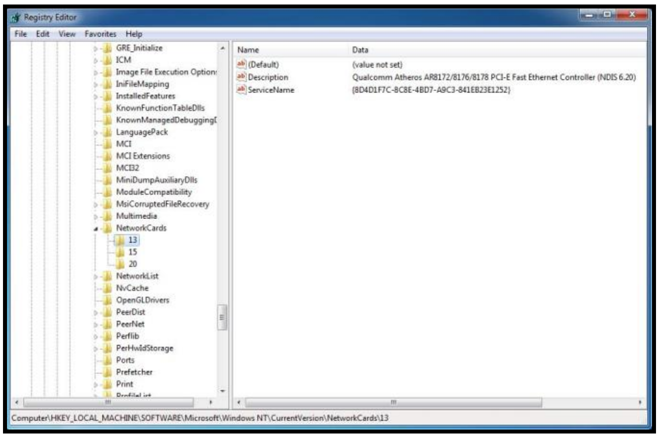
6) Goal and Objective

Investigator needs to have a good understanding of the registry keys as they provide significant and valuable information to perform a Registry examination. The keys related to system configuration, storage devices attached to the computer, resources and device drivers loaded when the system starts, user profiles, installed software and shortcuts provide important information. An investigator must be able to read hexadecimal values and convert them to readable text. Following are the registry keys in Windows 7 that are important to an investigator.

S.NO	Forensic Information	Windows Registry Key
1	Computer Name	HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control \ComputerName\ComputerName
2	BIOS Information	HKEY_LOCAL_MACHINE\ HARDWARE\DESCRIPTION\ System\BIOS
3	Last Shut Down Time of the System	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows
4	List of Startup Programs	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run
5	List of Registered Applications	HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications
6	Information about the network cards	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards
7	Information about the Wi-Fi Networks	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla \Wireless
8	List of USB Devices Connected till date	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR
9	List of Recently opened files and folders	HKEY_USERS\S-1-5-21-1905584886-2711141878-179018956-1000\Software\ Microsoft\ Windows\ CurrentVersion\Explorer\RecentDocs
10	List of Most recently typed command on the RUN Dialog	HKEY_USERS\S-1-5-21-1905584886-2711141878-179018956-1000\Software\ Microsoft\Windows\CurrentVersion\ Explorer\RunMRU

Here is a brief description of how network related information can be fetched from the windows registry.

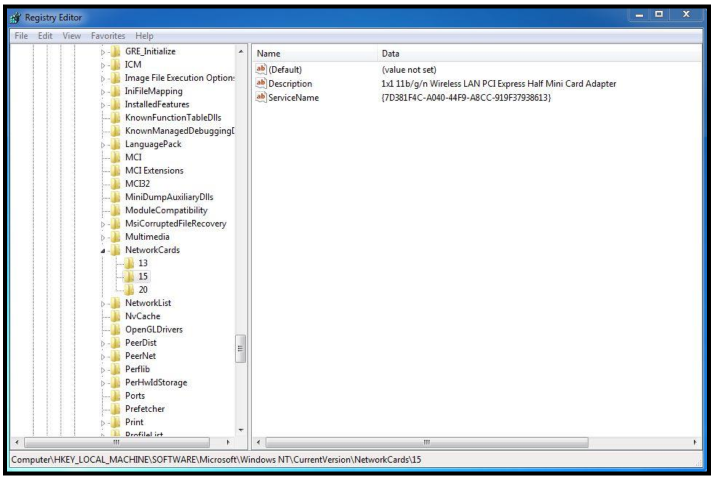
The Windows registry contains information about the network cards; no matter whether it is built-in or external Card. Normally card are of two types, either it can be a Ethernet card or it can be a Wi-Fi Network card. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\NetworkCards



Name	Data
(Default)	(value not set)
Description	Qualcomm Atheros AR8172/8176/8178 PCI-E Fast Ethernet Controller (NDIS 6.20)
ServiceName	{8D4D1F7C-8C8E-4BD7-A9C3-841EB23E1252}

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\13

Fig. 7 List of Network Cards (Ethernet)

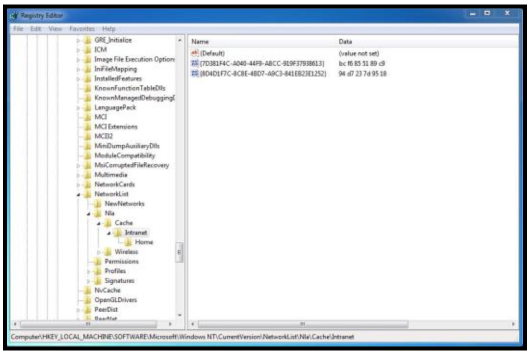


Name	Data
(Default)	(value not set)
Description	1x1 11b/g/n Wireless LAN PCI Express Half Mini Card Adapter
ServiceName	{7D381F4C-A040-44F9-A8CC-919F37938613}

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\15

Fig. 8 List of Network Cards (Wi-Fi)

In the same way, Windows Registry Contains information about the Intranet Network. HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\WindowsNT\CurrentVersion \NetworkList\Nla\Cache\Intranet

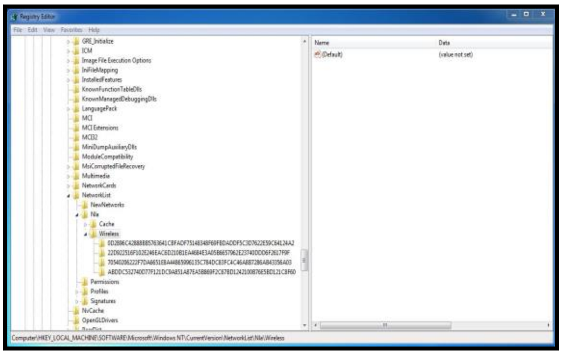


Name	Data
(Default)	(value not set)
{7D381F4C-A040-44F9-ABCC-919F37938613}	bc f6 85 51 89 c9
{8D4D1F7C-8C8E-4BD7-A9C3-841EB23E1252}	94 d7 23 7d 95 18

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache\Intranet

Fig. 9 List of Intranet in the Registry Keys

Information about the Wi-Fi Networks are listed here: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\ Network List\Nla\Wireless



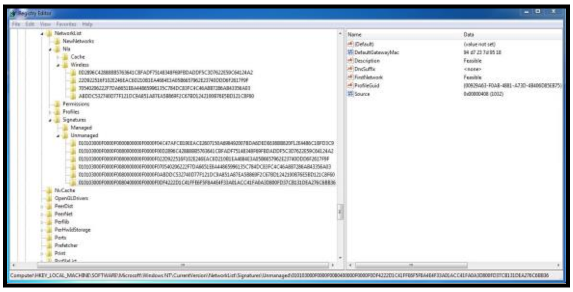
```
GRE_Initialize
ICM
Image File Execution Options
IniFileMapping
InstalledFeatures
KnownFunctionTableDlls
KnownManagedDebuggingDlls
LanguagePack
MCI
MCI Extensions
MCI32
MiniDumpAuxiliaryDlls
ModuleCompatibility
MsiCorruptedFileRecovery
Multimedia
NetworkCards
NetworkList
  NewNetworks
  Nla
    Cache
    Wireless
      0D2896C42888885763641CBFADF75148348F69FBDADDF5C3D7622E59C64124A2
      22D922516F102E246EAC6D210B1EA4684E3A05B6657962E23740DDD6F2617F9F
      70540206222F7DA6651EBA44865996135C784DC83FC4C46A887286AB43356A03
      ABDDC532740D77F121DC9A851A87EA5B869F2C678D1242100B76E5BD121C8F60
  Permissions
  Profiles
  Signatures
NvCache
OpenGLDrivers
```

Name	Data
(Default)	(value not set)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Wireless

Fig. 10 List of Wireless Network Identifiers

This key is just a list of identifiers for each of the wireless networks that the system has been connected to. More information about each of these wireless networks such as the MAC address of the default gateway, DNS suffix and SSID can also be found within the Registry. This can be done by linking the identifier from the previous key to the following Windows Registry key and is shown in Figure 11. This key holds a great deal of information about the networks in general rather than just about wireless networks. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ Network List\Signatures\Unmanaged



```
NetworkList
  NewNetworks
  Nla
    Cache
    Wireless
      0D2896C42888885763641CBFADF75148348F69FBDADDF5C3D7622E59C64124A2
      22D922516F102E246EAC6D210B1EA4684E3A05B6657962E23740DDD6F2617F9F
      70540206222F7DA6651EBA44865996135C784DC83FC4C46A887286AB43356A03
      ABDDC532740D77F121DC9A851A87EA5B869F2C678D1242100B76E5BD121C8F60
  Permissions
  Profiles
  Signatures
    Managed
    Unmanaged
      010103000F0000F0000800000F0000F04C47AFCB19EEACE2607150A6984920078DA6DED63888820F12E4486C18FD3C9
      010103000F0000F0080000000F0000F00D2896C42888885763641CBFADF75148348F69FBDADDF5C3D7622E59C64124A2
      010103000F0000F0080000000F0000F022D922516F102E246EAC6D210B1EA4684E3A05B6657962E23740DDD6F2617F9F
      010103000F0000F0080000000F0000F070540206222F7DA6651EBA44865996135C784DC83FC4C46A887286AB43356A03
      010103000F0000F0080000000F0000F0ABDDC532740D77F121DC9A851A87EA5B869F2C678D1242100B76E5BD121C8F60
      010103000F0000F0080400000F0000F0DF4222D1C41FFE8F5FBA4E4F33A01ACC41FA0A3D800FD37CB131DEA276C88B36
NvCache
OpenGLDrivers
PeerDist
PeerNet
Perflib
PerHwIdStorage
Ports
Prefetcher
Print
```

Name	Data
(Default)	(value not set)
DefaultGatewayMac	94 d7 23 7d 95 18
Description	Feasible
DnsSuffix	<none>
FirstNetwork	Feasible
ProfileGuid	{00929A63-F0AB-4881-A73D-48406D85EB75}
Source	0x00000408 (1032)

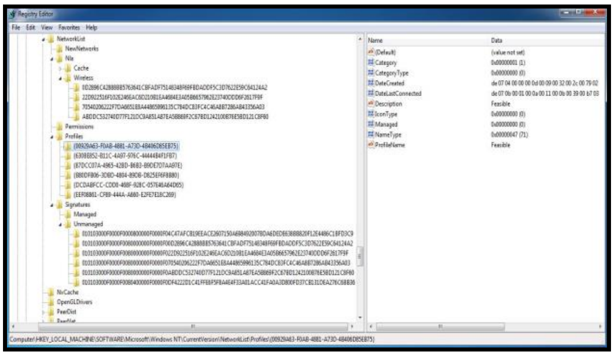
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged\010103000F0000F0080400000F0000F0DF4222D1C41FFE8F5FBA4E4F33A01ACC41FA0A3D800FD37CB131DEA276C88B36

Fig. 11 Matching Wireless network identifier

In addition, the Windows Registry holds important information for the forensic investigator about Wireless networks. This information includes the created date and last connected date.

They are stored in the following Registry sub key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles\{Wireless Identifiers}

The value DateCreated holds the created date of a specific wireless network and the value DateLastConnected holds the last date that the computer was connected to this wireless network as shown in Figure 12. The type of these values is binary data type. The following is an explanation how to view these values as a normal date time (Decoding the DateCreated and DateLastConnected SSID values From Vista/Win 7, 2010): The length of data of value is 16 bytes. It is stored using Little Endian, so convert it to big Endian before decoding the data as shown in Figure 13

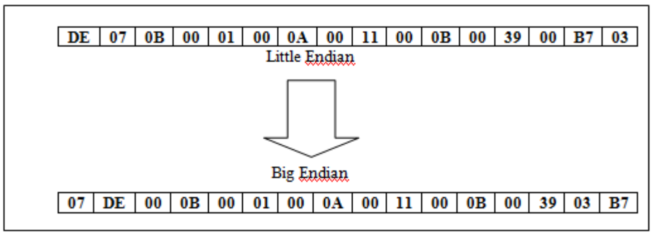


```
NetworkList
  NewNetworks
  Nla
    Cache
    Wireless
      0D2896C42888885763641CBFADF75148348F69FBDADDF5C3D7622E59C64124A2
      22D922516F102E246EAC6D210B1EA4684E3A05B6657962E23740DDD6F2617F9F
      70540206222F7DA6651EBA44865996135C784DC83FC4C46A887286AB43356A03
      ABDDC532740D77F121DC9A851A87EA5B869F2C678D1242100B76E5BD121C8F60
  Permissions
  Profiles
    {00929A63-F0AB-4881-A73D-48406D85EB75}
    {6308E852-B11C-4A97-976C-44444B4F1FB7}
    {87DCC07A-4965-428D-B6B3-89DE7D7AA97E}
    {880DFB06-3D8D-4804-89DB-D825EF6F8880}
    {DCDABFCC-CDD0-488F-928C-057E46A64D65}
    {EEF08861-CF89-444A-A680-E2FE7E18C269}
  Signatures
    Managed
    Unmanaged
      010103000F0000F0000800000F0000F04C47AFCB19EEACE2607150A6984920078DA6DED63888820F12E4486C18FD3C9
      010103000F0000F0080000000F0000F00D2896C42888885763641CBFADF75148348F69FBDADDF5C3D7622E59C64124A2
      010103000F0000F0080000000F0000F022D922516F102E246EAC6D210B1EA4684E3A05B6657962E23740DDD6F2617F9F
      010103000F0000F0080000000F0000F070540206222F7DA6651EBA44865996135C784DC83FC4C46A887286AB43356A03
      010103000F0000F0080000000F0000F0ABDDC532740D77F121DC9A851A87EA5B869F2C678D1242100B76E5BD121C8F60
      010103000F0000F0080400000F0000F0DF4222D1C41FFE8F5FBA4E4F33A01ACC41FA0A3D800FD37CB131DEA276C88B36
NvCache
OpenGLDrivers
PeerDist
PeerNet
```

Name	Data
(Default)	(value not set)
Category	0x00000001 (1)
CategoryType	0x00000000 (0)
DateCreated	de 07 04 00 00 00 0d 00 09 00 32 00 2c 00 79 02
DateLastConnected	de 07 0b 00 01 00 0a 00 11 00 0b 00 39 00 b7 03
Description	Feasible
IconType	0x00000000 (0)
Managed	0x00000000 (0)
NameType	0x00000047 (71)
ProfileName	Feasible

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{00929A63-F0AB-4881-A73D-48406D85EB75}

Fig. 12 Created date and last connected date of Wireless network



DE	07	0B	00	01	00	0A	00	11	00	0B	00	39	00	B7	03

Little Endian

Big Endian

07	DE	00	0B	00	01	00	0A	00	11	00	0B	00	39	03	B7

Fig. 13 Convert DateLastConnected Registry value to Big Endian format

- The year value = 07DE = 2014
- The month = 00 0B = 11=November (1= January, 2= February ...etc)
- Each two bytes has a corresponding value for the year, month, date, hour, minute and second.
- The weekday = 00 01 = Monday (0 = Sunday, 1 = Monday ...etc)
- The date = 00 0A = 10th
- The hour = 00 11 = 17:00 or 5:00 pm
- The minutes = 00 0B = 11 minutes
- The second = 00 39= 57 seconds
- Consequently, the decoded date is: Monday, 10th, November, 2014 17:11:57

IV. Result and Discussion

Start the forensic investigator tool by clicking on debugging option in Visual Studio 2010. The splash screen can be seen.

Fig. 14 Splash Screen

After Few seconds the main form gets started. The main form contains menus and sub-menus.

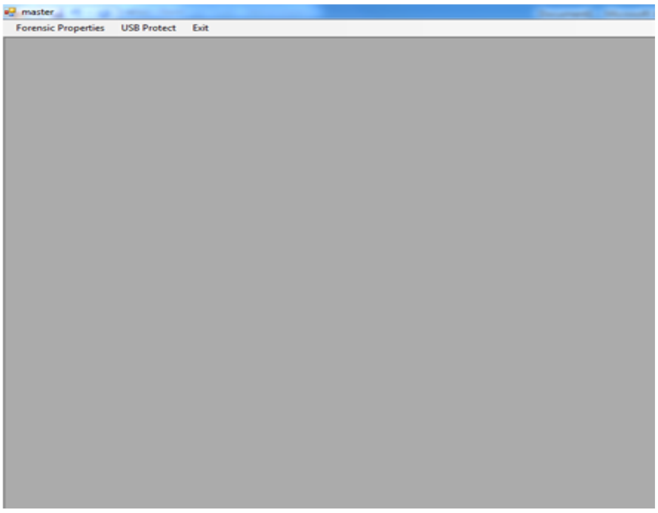


Fig. 15 Main Form

The main form menus contain the Items Forensic Analysis, USB Protect and Exit. The sub-menu is present only for the first menu item.

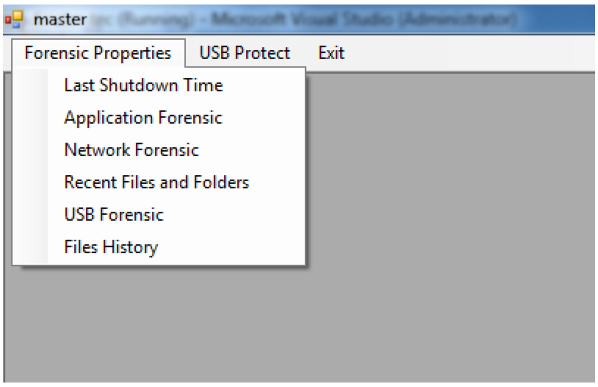
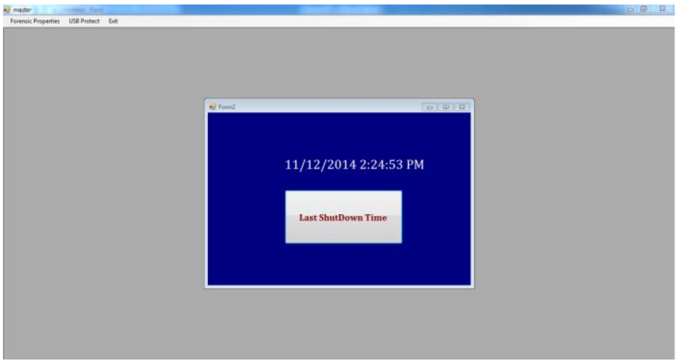


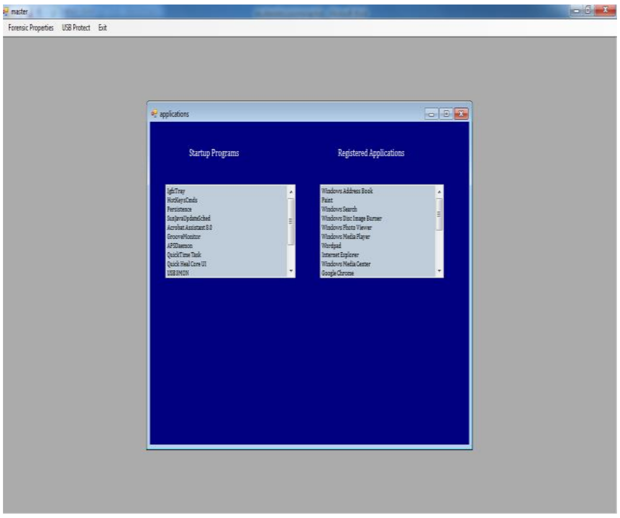
Fig. 16 Menus and Sub-Menus in the tool

The result of every sub-menu is show in the next pages. Firstly, lets consider the last shut down time option. The output is shown below. Similarly other forensics result can also be seen.



11/12/2014 2:24:53 PM

Fig. 17 Last Shut Down Time Output



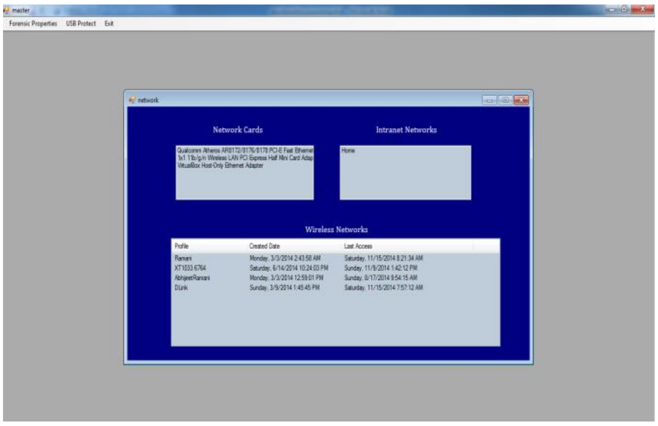
Startup Programs:

IgfxTray
HotKeysCmds
Persistence
SunJavaUpdateSched
Acrobat Assistant 8.0
GrooveMonitor
APSDaemon
QuickTime Task
Quick Heal Core UI
USB3MON

Registered Applications:

Windows Address Book
Paint
Windows Search
Windows Disc Image Burner
Windows Photo Viewer
Windows Media Player
Wordpad
Internet Explorer
Windows Media Center
Google Chrome

Fig. 18 Start up and Registered Application List



Network Cards:

Qualcomm Atheros AR8172/8176/8178 PCI-E Fast Ethernet
1x1 11b/g/n Wireless LAN PCI Express Half Mini Card Adap
VirtualBox Host-Only Ethernet Adapter

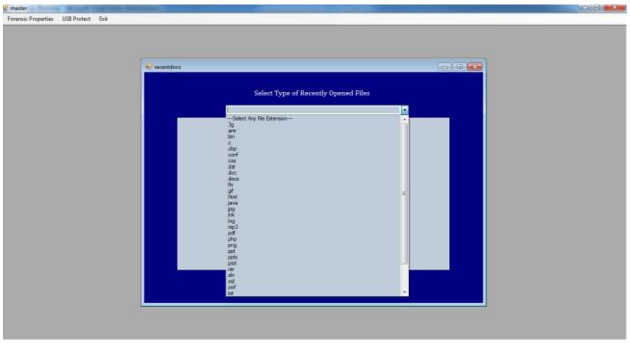
Intranet Networks:

Home

Wireless Networks:

Profile	Created Date	Last Access
Ramani	Monday, 3/3/2014 2:43:58 AM	Saturday, 11/15/2014 8:21:34 AM
XT1033 6764	Saturday, 6/14/2014 10:24:03 PM	Sunday, 11/9/2014 1:42:12 PM
AbhijeetRamani	Monday, 3/3/2014 12:59:01 PM	Sunday, 8/17/2014 9:54:15 AM
DLink	Sunday, 3/9/2014 1:45:45 PM	Saturday, 11/15/2014 7:57:12 AM

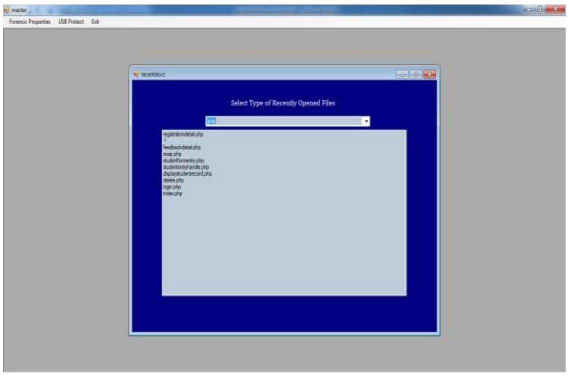
Fig. 19 Network Forensics



---Select Any File Extension---
.3g
.amr
.bin
.c
.cbp
.conf
.css
.dat
.doc
.docx
.flv
.gif
.html
.java
.jpg
.lnk
.log
.mp3
.pdf
.php
.png
.ppt
.pptx
.psd
.rar
.sln
.sql
.swf
.txt

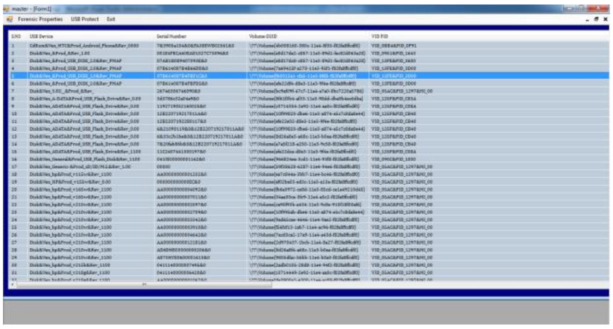
Fig. 20 Select List Item to get recently opened files and folder

Among the List of Items you can select any Item. The History for the selected file will be shown in the listview. The files can be with extensions c, php, doc, docx, jpg, png, gif, zip and many more.



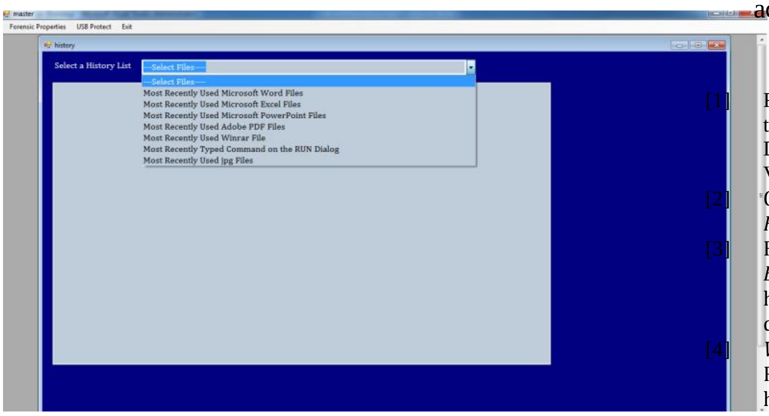
registrationdetail.php
1
feedbackdetail.php
swap.php
studentformentry.php
studententryhandle.php
displaystudentrecord.php
delete.php
login.php
index.php

Fig. 21 List of recently opened PHP files



S.NO	USB Device	Serial Number	Volume GUID	VID PID
1	CdRom&Ven_HTC&Prod_Android_Phone&Rev_0000	[illegible]	[illegible]	[illegible]
2	Disk&Ven_&Prod_&Rev_1.00	[illegible]	[illegible]	[illegible]
3	Disk&Ven_&Prod_USB_DISK_2.0&Rev_PMAP	[illegible]	[illegible]	[illegible]
4	Disk&Ven_&Prod_USB_DISK_2.0&Rev_PMAP	[illegible]	[illegible]	[illegible]
5	Disk&Ven_&Prod_USB_DISK_2.0&Rev_PMAP	[illegible]	[illegible]	[illegible]
6	Disk&Ven_&Prod_USB_DISK_2.0&Rev_PMAP	[illegible]	[illegible]	[illegible]
7	Disk&Ven_3.0_&Prod_&Rev_	[illegible]	[illegible]	[illegible]
8	Disk&Ven_A-DATA&Prod_USB_Flash_Drive&Rev_0.00	[illegible]	[illegible]	[illegible]
9	Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_0.00	[illegible]	[illegible]	[illegible]
10	Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_0.00	[illegible]	[illegible]	[illegible]
11	Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_0.00	[illegible]	[illegible]	[illegible]
12	Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_0.00	[illegible]	[illegible]	[illegible]
13	Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_0.00	[illegible]	[illegible]	[illegible]
14	Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_0.00	[illegible]	[illegible]	[illegible]
15	Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_1100	[illegible]	[illegible]	[illegible]
16	Disk&Ven_General&Prod_USB_Flash_Disk&Rev_1100	[illegible]	[illegible]	[illegible]
17	Disk&Ven_Generic-&Prod_[illegible]&Rev_1.00	00000	[illegible]	[illegible]
18	Disk&Ven_hp&Prod_v115w&Rev_1100	[illegible]	[illegible]	[illegible]
19	Disk&Ven_HP&Prod_v155w&Rev_0.00	[illegible]	[illegible]	[illegible]
20	Disk&Ven_hp&Prod_v165w&Rev_1100	[illegible]	[illegible]	[illegible]
21	Disk&Ven_hp&Prod_v165w&Rev_1100	[illegible]	[illegible]	[illegible]
22	Disk&Ven_hp&Prod_v210w&Rev_1100	[illegible]	[illegible]	[illegible]
23	Disk&Ven_hp&Prod_v210w&Rev_1100	[illegible]	[illegible]	[illegible]
24	Disk&Ven_hp&Prod_v210w&Rev_1100	[illegible]	[illegible]	[illegible]
25	Disk&Ven_hp&Prod_v210w&Rev_1100	[illegible]	[illegible]	[illegible]
26	Disk&Ven_hp&Prod_v210w&Rev_1100	[illegible]	[illegible]	[illegible]
27	Disk&Ven_hp&Prod_v210w&Rev_1100	[illegible]	[illegible]	[illegible]
28	Disk&Ven_hp&Prod_v210w&Rev_1100	[illegible]	[illegible]	[illegible]
29	Disk&Ven_hp&Prod_v210w&Rev_1100	[illegible]	[illegible]	[illegible]
30	Disk&Ven_hp&Prod_v215b&Rev_1100	[illegible]	[illegible]	[illegible]
31	Disk&Ven_hp&Prod_v215g&Rev_1100	[illegible]	[illegible]	[illegible]

Fig. 22 USB Forensics



---Select Files---
Most Recently Used Microsoft Word Files
Most Recently Used Microsoft Excel Files
Most Recently Used Microsoft PowerPoint Files
Most Recently Used Adobe PDF Files
Most Recently Used Winrar File
Most Recently Typed Command on the RUN Dialog
Most Recently Used jpg Files

Fig. 23 History of some commonly used files

V. CONCLUSIONS AND FUTURE SCOPE

Windows and every program that runs on windows operating system environment gets execute only after consulting the windows registry. Windows registry is one of the finest ways of initial investigation in the field of computer or digital forensic analysis. The ultimate target goal is to fetch the forensic information and decode it to examine the footprints left after any type of criminological activity caused intentionally or unintentionally.

With an aim to make the forensic investigation easier, a tool was implemented with reduces time and increase the forensic output efficiency. Mostly, all the keys and sub-keys discussed so far, has been implemented in the forensic tool.

The present research deals with limited area of windows registry keys in the investigation process. Therefore, the present research can be upgraded and new solutions can be identified which will be very helpful in performing forensic analysis easily.

Forensic Analysis on Windows 8 and higher operating system can be carried out. An application to detect quickly the MAC time of various files in a directory. Also the user should have a provision to select a particular directory for finding out the MAC times. All this MAC timestamps in combination with information obtained from USB forensics can be very useful for forensics analysis.

A key-logger background process can be developed which records the LIVE activities information to understand the working pattern and signature of users and hackers. This signature shall be very useful in developing strong and reliable forensic tools. Also, the data obtained from the key-logger can be used to draw the timeline of actions. Searching with time could be a useful module.

In this era of globally distributed technology anyone from anywhere can access their information. It would be a wonderful idea to implement a forensic investigation approach to analyze windows registry remotely.

An efficient approach can be carried to detect various Malware and intruders carrying out unwanted events and activities.

REFERENCES

[1] Ramani, A & Dewangan, S (2014). Auditing Windows 7 Registry Keys to track the traces left out in copying files from system to external USB Device. Retrieved August,2014, from http://www.ijcsit.com/docs/ Volume%205/ vol5issue02/ijcsit2014050220.pdf

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

[3] Farmer, D.J.(n.d.). *A windows registry Quick Reference: For the Everyday Examiner*. Retrieved December, 2013, from http://www.forensicfocus.com/downloads/windows-registry-quick-reference.pdf

[4] *Windows registry information for advanced users*. Retrieved December 2013, from Microsoft Support. http://support.microsoft.com/kb/256986

[5] Barbara, J.J.(2011).*Windows 7 Registry Forensics*. Retrieved January, 2014, from http://www.forensicmag.com/articles/2012/ 06/windows-7-registry-forensics-part-5#.Uv-TkPtfaSo

[6] Wong, L.W.(n. d.).*Forensic Analysis of Windows Registry*. Retrieved January, 2014, from http://www.forensictv.net/Downloads /digital_forensics/forensic_analysis_of_windows_registry_by_lih_wern_wong.pdf

[7] Jain, A & Roy, T.(2012).*Windows Registry Forensics: An Imperative Step in Tracking Data Theft via USB Devices*. Retrieved January, 2014, from http://www.ijcsit.com/docs/Volume%203/vol3Issue3/ ijcsit20120303126.pdf

[8] Alghafli, K.A & Jones, A & Martin T.A. (2010) .*Forensic Analysis of the Windows 7 Registry*. Retrieved Retrieved January, 2014, from Edith Cawan University Research online. http://ro.ecu.edu.au/cgi/ viewcontent.cgi?article=1071&context=adf

[9] Fisher, T. (n.d.). *Windows Registry*. Retrieved January, 2014, from http://pcsupport.about.com/od/termsr/p/registrywindows.htm

[10] Fisher, T. (n.d.). *Registry Hives*. Retrieved January, 2014, from http://pcsupport.about.com/od/termsr/g/registryhive.htm

[11] Fisher, T. (n.d.). *HKEY_CLASSES_ROOT* Retrieved January, 2014, from http://pcsupport.about.com/od/termshm/g/hkey classes root.htm

[12] Fisher, T. (n.d.). *HKEY_CURRENT_USER*. Retrieved January, 2014, fromhttp://pcsupport.about.com/od/termshm/g/hkey current user.htm

[13] Fisher, T. (n.d.). *HKEY_LOCAL_MACHINE*. Retrieved January, 2014, from http://pcsupport.about.com/od/termshm/g/hkey local machine.htm

[14] Fisher, T. (n.d.). *HKEY_USERS*. Retrieved January, 2014, from http://pcsupport.about.com/od/termshm/g/hkey users.htm

[15] Fisher, T. (n.d.). *HKEY_CURRENT_CONFIG.* Retrieved January, 2014 from http://pcsupport.about.com/od/termshm/g/hkey current config.htm

[16] Liming Cai & Jing Sha & Wei Qian (2013). Study on Forensic Analysis of Physical Memory. Retrieved March 2014 from www.atlantis-press.com/php/download_ paper.php?id=10172

[17] Haoyang Xie & Keyu Jiang Xiaohong Yuan & Hongbiao Zeng (2012). Forensic Analysis of Windows Registry Against Intrusion. Retrieved July 2014 from http://caeiae.ncat.edu/Forensic%20Analysis%20of%20 Windows %20Registry%20Against%20Intrusion.pdf

[18] Lih Wern Wong (n.d.).Forensic Analysis of the Windows Registry.Retrieved July 2014 From https://www.scribd.com/doc/2251 55972/Forensic-Analysis-of-Windows-Registry-by-Lih-Wern-Wong

[19] Yuri Gubanov (2012).Retrieving Digital Evidence: Methods, Techniques and Issues.Retrieved on July 2014 From http://forensic.belkasoft.com /en/retrieving-digital-evidence-methods-techniques-and-issues

[20] Jerry Honeycutt (2005).Microsoft Windows Registry Guide 2nd Edition. Retrieved on october 2014 from https://www.it-ebooks.info.

[21] "msdn.microsoft" [Online] Available: http://msdn.microsoft.com/en-us/library/windows/desktop /ms7248 71%28v=vs.85%29.aspx

[22] "msdn.microsoft" [Online] Available:http://msdn.microsoft.com/en-us/library/windows/desktop/ ms7248 77%28v=vs.85%29.aspx

[23] "support.microsoft" [Online] Available:http://support.microsoft.com/kb/256986/en-us/

[24] "sqlcoffee" [Online] Available:Available:http://www.sqlcoffee.com/troubleshooting051.htm "gaurangpatel" [Online]

[25] Available:http://gaurangpatel.net/sql-server-installation-rules-and-system- reboot-required-error

[26] "microsoft" [Online] Available:http://www.microsoft.com/en-in/download/details.aspx? id=23691

[27] "msdn.microsoft" [Online] Available:http://msdn.microsoft.com/en-us/library/w0x726c2 (v=vs.100).aspx

[28] "msdn.microsoft" [Online] Available:http://msdn.microsoft.com/en-us/library/ff361664 (v=vs.110).aspx

[29] "msdn.microsoft" [Online] Available:http://msdn.microsoft.com/en-us/library/gg14501 1(v=vs.100).aspx

[30] "msdn.microsoft" [Online] Available:http://msdn.microsoft.com/en-us/library/Microsoft.Win32 (v=vs.100).aspx

[31] "msdn.microsoft" [Online] Available:http://msdn.microsoft.com/en-us/library/aa289494 (v=vs.71).aspx

[32] "msdn.microsoft" [Online] Available:http://msdn.microsoft.com/en-us/library/microsoft.win32. registry(v=vs.71).aspx

[33] "msdn.microsoft" [Online] Available:http://msdn.microsoft.com/en-us/library/microsoft.win32. registrykey(v=vs.100).aspx

[34] "msdn.microsoft" [Online] Available:http://msdn.microsoft.com/en-us/library/z9f66s0a (v=vs.100).aspx

[35] "msdn.microsoft" [Online] Available:http://msdn.microsoft.com/en-us/library/8zha3xws (v=vs.110).aspx

[36] "msdn.microsoft" [Online] Available:http://msdn.microsoft.com/en-us/library/gg265786 (v=vs.100).aspx

First Author: *Abhijeet Ramani*, received his Bachelor of Engineering degree in Computer Science & Engineering from Disha Institute of Mangement and Technology, Raipur, Chhattisgarh, INDIA, Chhattisgarh Swami Vivekananda Technical University (CSVTU) Bhilai, in 2011. He is currently an M.Tech student in the Computer Science & Engineering from Disha Institute of Mangement and Technology, Raipur, Chhattisgarh, INDIA, Chhattisgarh Swami Vivekananda Technical University (CSVTU) Bhilai. His research interests include Information Security & Cryptography, Software Development, Web Development, Android Mobile Apps Development, Embedded Systems & Robotics, and Software Testing & Deployment.

Second Author: *Somesh Kumar Dewangan* received his M.Tech in Computer Science and Engineering from RCET Bhilai, Chhattisgarh Swami Vivekananda University Bhilai , in 2009. Before that the MCA. Degree in Computer Application from MPBO University, Bhopal, India, in 2005. He is lecturer, Assistant Professor, Associate professor, Disha Institute of Management and Technology, Chhattisgarh Swami Vivekananda Technical University Bhilai, India, in 2005 and 2008 respectively. His research interests include digital signal processing and image processing, Natural Language Processing, Neural Network, Artificial Intelligence, Information & Network Security, mo bile Networking and Cryptography & Android based Application.