ISSN:0975-9646

Auditing Windows 7 Registry Keys to track the traces left out in copying files from system to external USB Device

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— **Today in the world of big data, information is critical and corporate professional firms are adopting the digital forensic technique for detecting the action timeline of the activities carried out. Digital forensics is an important subdivision of data and network security. With the increase in technology, attacks on data are also increasing. It is very difficult to cultivate the methods for maintaining the CIA (Confidentiality, Integrity & Authenticity) security principles. In this paper, we describe the importance of the study on computer & digital forensics. 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 the copying of data into external flash drives, such as an USB storage device. Windows registry forensic keys can be applied in carrying the investigation process. For the sake of simplicity, there will only be the reference to the windows 7 operating system. Our main focus will be on to track the identification of files that might have been copied into external USB mass drives in the absence of the legitimate user. Also, we will also see that if certain registry key values are modified then the functionality behaves differently. This paper will briefly introduce the windows 7 registry structure which is very useful for the forensics expert to carry out digital forensic analysis.**

Keywords—**Windows Registry, Windows 7 Forensic Analysis, Windows Registry Structure, Analysing Registry Key, Tracking Copying of data from system to USB.**

I. Introduction

Few months back, while installing SQLSERVER 2008, a message was found-“Windows Restart Required”. After restarting, the same message was found again. The things were really getting very tedious. What to do?? After Continuous hunting for the solution, finally a method was obtained. It shown the resolving of the error can be done by erasing some data from windows registry keys- “Pending File Operations”. After erasing, the setup was run again under the option “Re-run” and it was really wonderful to see that now the installation process was not asking for Re-start. It was something made to think how really the things have worked. What actually is the Windows Registry? What functionality it does? What are the attributes of Windows Registry? This paper is all about the research carried out to know windows registry in depth. Can forensic methods be applied on windows registry, for discovering the hidden information? According to Microsoft Knowledge Base (KB) article 256986 [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.

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 algorithm for tracking the data transfer from system to USB device. 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 [1] 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 [2] 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".

Alghafli, K.A. & Jones, A. & Martin, T.A. [7] 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.

Jain, A. & Roy, T. [6] have conducted their research on Windows XP Registry structure. In this paper importance of Windows XP Registry structure was explained with an enhancement to track data theft from system to USB external devices. Here analysis was done on a suspected file to identify its timestamps. But the research was not carried for the Windows 7 Registry Structure.

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

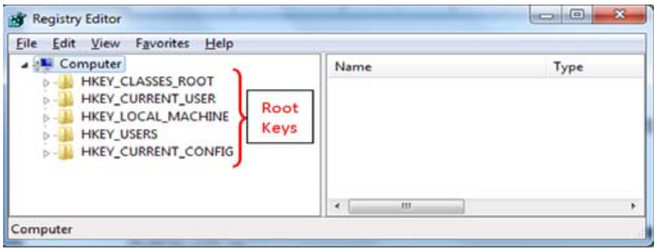


Fig. 1 Windows Registry root Keys

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:

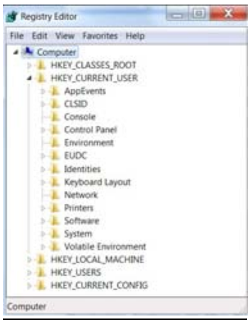


Fig. 2 HKEY_CURRENT_USERS Keys

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:

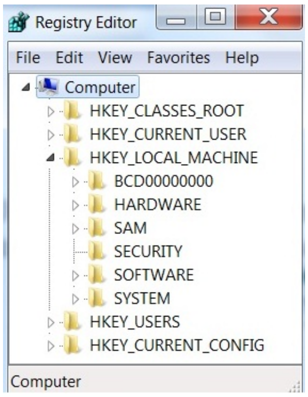


Fig. 3 HKEY_LOCAL_MACHINE Keys

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.

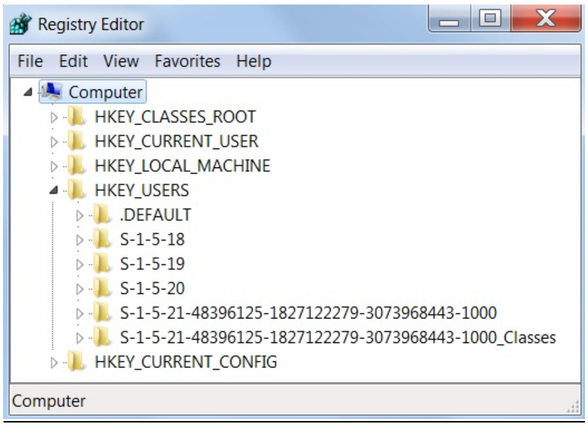
"21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx" is the domain or local computer identifier. (Note: The numbering schema "xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx" will differ from computer to computer since it corresponds to individual, unique User accounts).

"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:

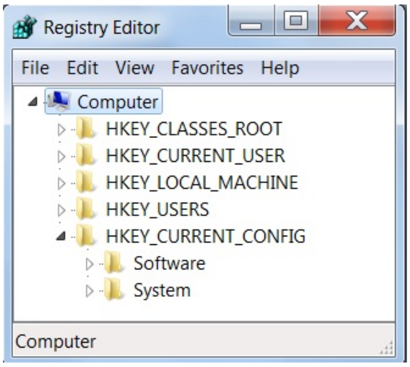


Computer
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
  - .DEFAULT
  - S-1-5-18
  - S-1-5-19
  - S-1-5-20
  - S-1-5-21-48396125-1827122279-3073968443-1000
  - S-1-5-21-48396125-1827122279-3073968443-1000_Classes
- HKEY_CURRENT_CONFIG

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:



Computer
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG
  - Software
  - System

Fig. 5 HKEY_CURRENT_CONFIG Keys

3) *Algorithm & Procedure:*

Before discussing about the method will be using in detecting whether there is a data transfer from suspected file to external USB drive. Let us discuss about the MAC (Modified, Accessed, and Created) timestamps. Each file in a system is associated with the MAC time. It can be a text file, word file, image file, database file, webpage file and many more. Whenever any file is copied or moved or opened then their accessed time gets changed. Also, if any changes have been done in the file then both modified & accessed time gets changed. Created time comes to play at the time when a file is created. Forensic analysis of these timestamps can result in finding out many hidden information necessary for achieving security.

Every device contains various device parameters, such as, vendor Id, Product Id, Serial Number, Version, Parent Id Prefix etc. Also each device when gets plugged into the system is associated with some extra parameters such as GUIDs (Global Universal Identifier), Unique identifiers etc. In forensic analysis we need to collect information about these parameters and later, on the basis of values obtained we conclude with some results. Below are the steps involved for forensic analysis-

a) Identify the file which is suspected of being copied. Let us take a very crucial database file which contains the list of customers, say, customers.sql.

b) Right click on the file and go to properties. Note down the MAC time.

c) Find out the Vendor Id, Product Id & Version
SYSTEM*CurrentControlSet*\Enum\USBSTOR

d) Find out the serial number
SYSTEM*CurrentControlSet*\Enum\USBSTOR

e) Determine Parent Prefix ID
SYSTEM*CurrentControlSet*\Enum\USBSTOR

f) **Determine the drive Letter were the Device was Mapped**
SYSTEM\MountedDevices-Perform Search for Parent Prefix ID

g) Identify the Volume GUIDs
SYSTEM\MountedDevices- Perform Search for Parent Prefix ID

h) Find out the user that used the specific USB Device
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2- Search for Device GUID

i) Determine the last time device was connected.
SYSTEM*CurrentControlSet*\Control\DeviceClasses \{53f56307-b6bf-11d0-94f2-00a0c91efb8b}- Perform search for Serial Number

j) **Identify the first time device was Connected**

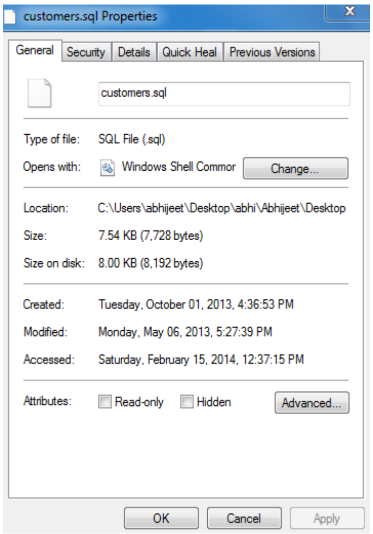
Whenever a flash drive is connected for the first time in the system, all its event is recorded in the file (setupai.dev.log).

Search on the basis of device serial number

C:\Windows\inf\setupapi.dev.log

IV. Result and Discussion

Step 1: Identify the MAC (Modified, Accessed, Creation) time of the suspected file customers.sql



customers.sql Properties

customers.sql

Type of file: SQL File (.sql)

Opens with: Windows Shell Commor

Location: C:\Users\abhijeet\Desktop\abhi\Abhijeet\Desktop

Size: 7.54 KB (7,728 bytes)

Size on disk: 8.00 KB (8,192 bytes)

Created: Tuesday, October 01, 2013, 4:36:53 PM

Modified: Monday, May 06, 2013, 5:27:39 PM

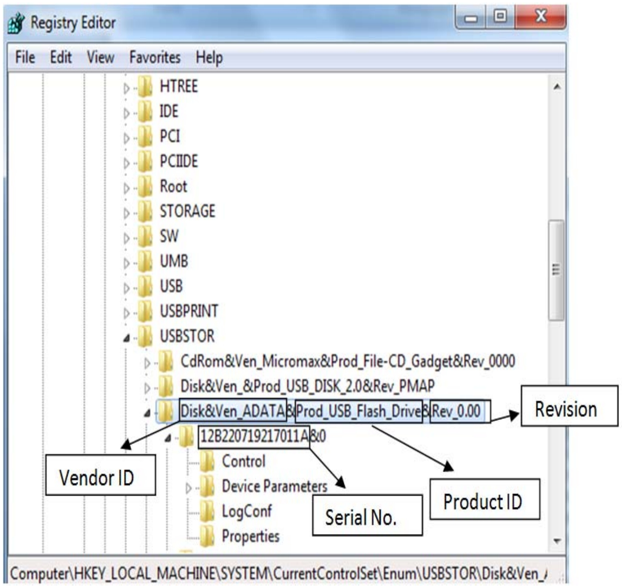
Accessed: Saturday, February 15, 2014, 12:37:15 PM

Attributes: □ Read-only □ Hidden

Fig. 6 MAC timestamps of customers.sql

Step 2: Start the Registry Editor (regedit) and write down the Vendor, Product, Version, Serial Number, and Parent-Prefix-ID

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Enum/USBSTOR

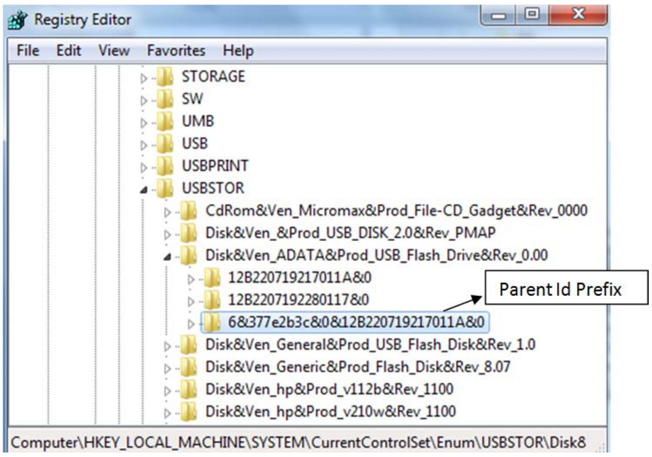


Registry Editor

```
HTREE
IDE
PCI
PCIIDE
Root
STORAGE
SW
UMB
USB
USBPRINT
USBSTOR
  CdRom&Ven_Micromax&Prod_File-CD_Gadget&Rev_0000
  Disk&Ven_&Prod_USB_DISK_2.0&Rev_PMAP
  Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_0.00
    12B220719217011A&0
      Control
      Device Parameters
      LogConf
      Properties
```

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_/

Fig. 7 Identification of Device Parameters



Registry Editor

```
STORAGE
SW
UMB
USB
USBPRINT
USBSTOR
  CdRom&Ven_Micromax&Prod_File-CD_Gadget&Rev_0000
  Disk&Ven_&Prod_USB_DISK_2.0&Rev_PMAP
  Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_0.00
    12B220719217011A&0
    12B2207192280117&0
    6&377e2b3c&0&12B220719217011A&0
  Disk&Ven_General&Prod_USB_Flash_Disk&Rev_1.0
  Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07
  Disk&Ven_hp&Prod_v112b&Rev_1100
  Disk&Ven_hp&Prod_v210w&Rev_1100
```

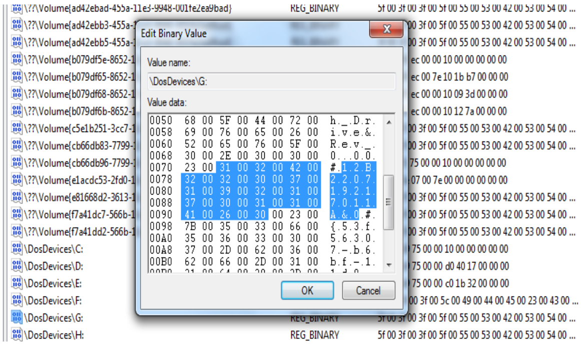
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk8

Fig. 8 Identification of Parent Id Prefix

Step 3: Determine Drive Letter where the device was mapped to, on the basis of Serial Number obtained from step 2.It is clear Fig. 10 that, the device was mapped into drive G.

HKEY_LOCAL_MACHINE/SYSTEM/MountedDevices

Fig. 9 Right hand side consist of list of GUIDS (Global Unique Identifier)



```
\??\Volume{ad42ebad-455a-11e3-9948-001fe2ea9bad}   REG_BINARY   5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{ad42ebb3-455a-1                                      00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{ad42ebb5-455a-1                                      00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{b079df5e-8652-1                                      ec 00 00 10 00 00 00 00 00
\??\Volume{b079df65-8652-1                                      ec 00 7e 10 1b b7 00 00 00
\??\Volume{b079df68-8652-1                                      ec 00 00 10 09 3d 00 00 00
\??\Volume{b079df6b-8652-1                                      ec 00 00 10 12 7a 00 00 00
\??\Volume{c5e1b251-3cc7-1                                      00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{cb66db83-7799-1                                      00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{cb66db96-7799-1                                      75 00 00 10 00 00 00 00 00
\??\Volume{e1acdc53-2fd0-1                                      07 00 7e 00 00 00 00 00 00
\??\Volume{e81668d2-3613-1                                      00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{f7a41dc7-566b-1                                      00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{f7a41dd2-566b-1                                      00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\DosDevices\C:                                                  75 00 00 10 00 00 00 00 00
\DosDevices\D:                                                  75 00 00 d0 40 17 00 00 00
\DosDevices\E:                                                  75 00 00 c0 1b 32 00 00 00
\DosDevices\F:                                                  00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 ...
\DosDevices\G:                                 REG_BINARY       5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\DosDevices\H:                                 REG_BINARY       5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
```

Edit Binary Value

Value name: \DosDevices\G:

Value data:

```
0050   68 00 5F 00 44 00 72 00   h._.D.r.
0058   69 00 76 00 65 00 26 00   i.v.e.&.
0060   52 00 65 00 76 00 5F 00   R.e.v._.
0068   30 00 2E 00 30 00 30 00   0...0.0.
0070   23 00 31 00 32 00 42 00   #.1.2.B.
0078   32 00 32 00 30 00 37 00   2.2.0.7.
0080   31 00 39 00 32 00 31 00   1.9.2.1.
0088   37 00 30 00 31 00 31 00   7.0.1.1.
0090   41 00 26 00 30 00 23 00   A.&.0.#.
0098   7B 00 35 00 33 00 66 00   {.5.3.f.
00A0   35 00 36 00 33 00 30 00   5.6.3.0.
00A8   37 00 2D 00 62 00 36 00   7.-.b.6.
00B0   62 00 66 00 2D 00 31 00   b.f.-.1.
```

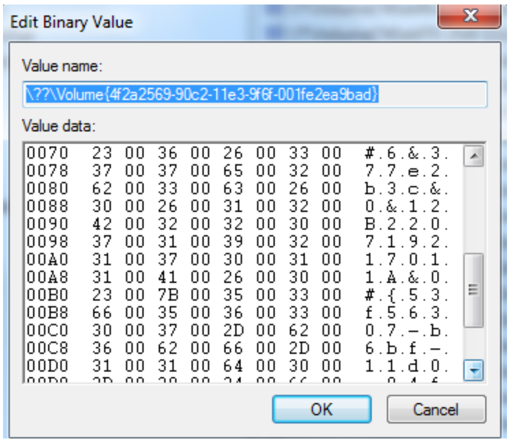
Fig. 10 Serial Number obtained from the Volume GUID List

Step 4: Identify the Volume GUIDS on the basis of Serial number.

HKEY_LOCAL_MACHINE/SYSTEM/MountedDevices

On Right Hand Side, Click on each Name entry to search for the Parent Id Prefix GUIDs for each device are listed as "\??\Volume{xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx}."

You may find more than one GUIDs.



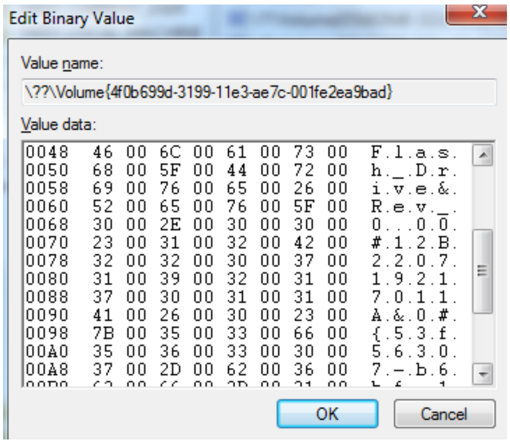
Value name:

\??\Volume{4f2a2569-90c2-11e3-9f6f-001fe2ea9bad}

Value data:

```
0070   23  00  36  00  26  00  33  00   #.6.&.3.
0078   37  00  37  00  65  00  32  00   7.7.e.2.
0080   62  00  33  00  63  00  26  00   b.3.c.&.
0088   30  00  26  00  31  00  32  00   0.&.1.2.
0090   42  00  32  00  32  00  30  00   B.2.2.0.
0098   37  00  31  00  39  00  32  00   7.1.9.2.
00A0   31  00  37  00  30  00  31  00   1.7.0.1.
00A8   31  00  41  00  26  00  30  00   1.A.&.0.
00B0   23  00  7B  00  35  00  33  00   #.{.5.3.
00B8   66  00  35  00  36  00  33  00   f.5.6.3.
00C0   30  00  37  00  2D  00  62  00   0.7.-.b.
00C8   36  00  62  00  66  00  2D  00   6.b.f.-.
00D0   31  00  31  00  64  00  30  00   1.1.d.0.
```

Fig. 11 First GUID obtained



Value name:

\??\Volume{4f0b699d-3199-11e3-ae7c-001fe2ea9bad}

Value data:

```
0048   46  00  6C  00  61  00  73  00   F.l.a.s.
0050   68  00  5F  00  44  00  72  00   h._.D.r.
0058   69  00  76  00  65  00  26  00   i.v.e.&.
0060   52  00  65  00  76  00  5F  00   R.e.v._.
0068   30  00  2E  00  30  00  30  00   0...0.0.
0070   23  00  31  00  32  00  42  00   #.1.2.B.
0078   32  00  32  00  30  00  37  00   2.2.0.7.
0080   31  00  39  00  32  00  31  00   1.9.2.1.
0088   37  00  30  00  31  00  31  00   7.0.1.1.
0090   41  00  26  00  30  00  23  00   A.&.0.#.
0098   7B  00  35  00  33  00  66  00   {.5.3.f.
00A0   35  00  36  00  33  00  30  00   5.6.3.0.
00A8   37  00  2D  00  62  00  36  00   7.-.b.6.
```

Fig. 12 Second GUID obtained

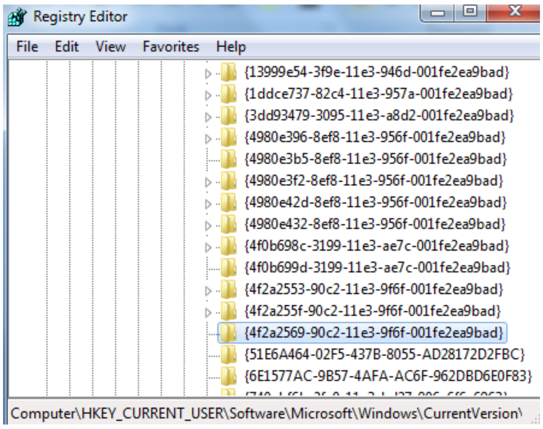
Step 5: Find the User Profile that used the specific USB device on the basis of device GUID.

In the last step we have obtained GUID as:

\??\Volume{4f2a2569-90c2-11e3-9f6f-001fe2ea9bad}
and
\??\Volume{4f0b699d-3199-11e3-ae7c-001fe2ea9bad}
HKEY_CURRENT_USER\Software\Microsoft\Windows \CurrentVersion\Explorer\MountPoints2

We obtained:

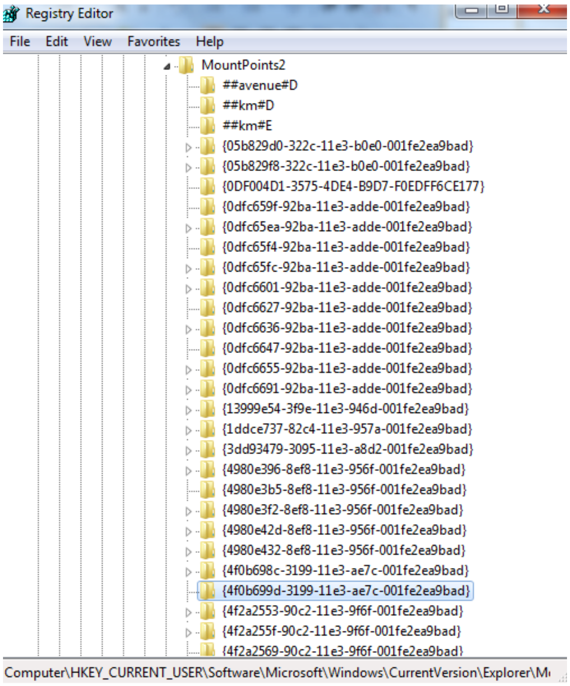
HKEY_CURRENT_USER\Software\Microsoft\Windows \CurrentVersion\Explorer\MountPoints2\{4f2a2569-90c2-11e3-9f6f-001fe2ea9bad}



```
{13999e54-3f9e-11e3-946d-001fe2ea9bad}
{1ddce737-82c4-11e3-957a-001fe2ea9bad}
{3dd93479-3095-11e3-a8d2-001fe2ea9bad}
{4980e396-8ef8-11e3-956f-001fe2ea9bad}
{4980e3b5-8ef8-11e3-956f-001fe2ea9bad}
{4980e3f2-8ef8-11e3-956f-001fe2ea9bad}
{4980e42d-8ef8-11e3-956f-001fe2ea9bad}
{4980e432-8ef8-11e3-956f-001fe2ea9bad}
{4f0b698c-3199-11e3-ae7c-001fe2ea9bad}
{4f0b699d-3199-11e3-ae7c-001fe2ea9bad}
{4f2a2553-90c2-11e3-9f6f-001fe2ea9bad}
{4f2a255f-90c2-11e3-9f6f-001fe2ea9bad}
{4f2a2569-90c2-11e3-9f6f-001fe2ea9bad}
{51E6A464-02F5-437B-8055-AD28172D2FBC}
{6E1577AC-9B57-4AFA-AC6F-962DBD6E0F83}
```

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\

Fig. 13 First GUID Matched



```
MountPoints2
    ##avenue#D
    ##km#D
    ##km#E
    {05b829d0-322c-11e3-b0e0-001fe2ea9bad}
    {05b829f8-322c-11e3-b0e0-001fe2ea9bad}
    {0DF004D1-3575-4DE4-B9D7-F0EDFF6CE177}
    {0dfc659f-92ba-11e3-adde-001fe2ea9bad}
    {0dfc65ea-92ba-11e3-adde-001fe2ea9bad}
    {0dfc65f4-92ba-11e3-adde-001fe2ea9bad}
    {0dfc65fc-92ba-11e3-adde-001fe2ea9bad}
    {0dfc6601-92ba-11e3-adde-001fe2ea9bad}
    {0dfc6627-92ba-11e3-adde-001fe2ea9bad}
    {0dfc6636-92ba-11e3-adde-001fe2ea9bad}
    {0dfc6647-92ba-11e3-adde-001fe2ea9bad}
    {0dfc6655-92ba-11e3-adde-001fe2ea9bad}
    {0dfc6691-92ba-11e3-adde-001fe2ea9bad}
    {13999e54-3f9e-11e3-946d-001fe2ea9bad}
    {1ddce737-82c4-11e3-957a-001fe2ea9bad}
    {3dd93479-3095-11e3-a8d2-001fe2ea9bad}
    {4980e396-8ef8-11e3-956f-001fe2ea9bad}
    {4980e3b5-8ef8-11e3-956f-001fe2ea9bad}
    {4980e3f2-8ef8-11e3-956f-001fe2ea9bad}
    {4980e42d-8ef8-11e3-956f-001fe2ea9bad}
    {4980e432-8ef8-11e3-956f-001fe2ea9bad}
    {4f0b698c-3199-11e3-ae7c-001fe2ea9bad}
    {4f0b699d-3199-11e3-ae7c-001fe2ea9bad}
    {4f2a2553-90c2-11e3-9f6f-001fe2ea9bad}
    {4f2a255f-90c2-11e3-9f6f-001fe2ea9bad}
    {4f2a2569-90c2-11e3-9f6f-001fe2ea9bad}
```

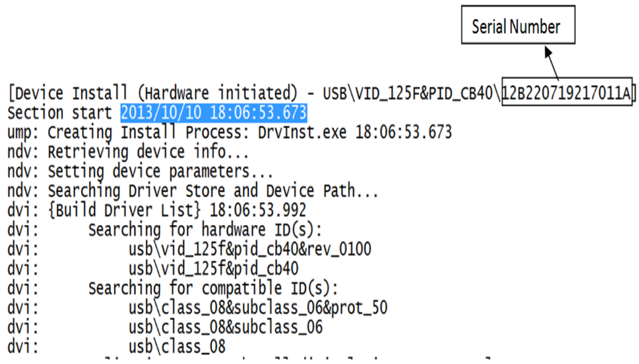
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\M

Fig. 14 Second GUID Matched

Both the GUIDS entry was have found here and is for the user "abhijeet" (as currently logged in with username "abhijeet"). Therefore, this is confirm that the device was plug in from the user account "abhijeet"

Step 6: Discover the first time, the device was connected. For this, the setupapi.dev.log file is investigated. When ever a flash drive is connected for the first time in the system, all its event is recorded in this file. Search on the basis of Device serial number

C:\Windows\inf\setupapi.dev.log



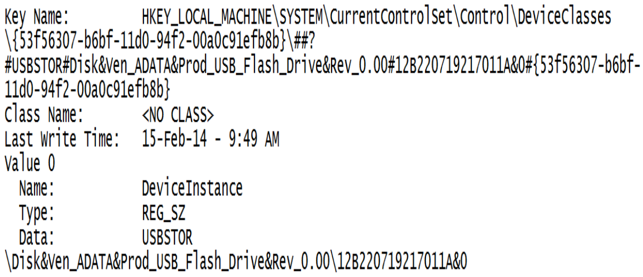
```
[Device Install (Hardware initiated) - USB\VID_125F&PID_CB40\12B220719217011A]
Section start 2013/10/10 18:06:53.673
ump: Creating Install Process: DrvInst.exe 18:06:53.673
ndv: Retrieving device info...
ndv: Setting device parameters...
ndv: Searching Driver Store and Device Path...
dvi: {Build Driver List} 18:06:53.992
dvi:      Searching for hardware ID(s):
dvi:           usb\vid_125f&pid_cb40&rev_0100
dvi:           usb\vid_125f&pid_cb40
dvi:      Searching for compatible ID(s):
dvi:           usb\class_08&subclass_06&prot_50
dvi:           usb\class_08&subclass_06
dvi:           usb\class_08
```

Fig. 15 Snapshot of setupapi.dev.log. Here the time can be seen when device was connected for the first date & time. The format of date is yyyy/mm/dd

Step 7: Determine first time device connected after last reboot on the basis of serial number. Right Click here and export to text file and search for last write time.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?#USBSTOR#Disk&Ven_ADATA&Pro

d_USB_Flash_Drive&Rev_0.00#12B220719217011A&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

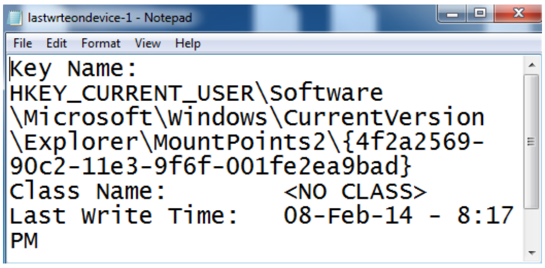


```
Key Name:        HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses
\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\##?
#USBSTOR#Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_0.00#12B220719217011A&0#{53f56307-b6bf-
11d0-94f2-00a0c91efb8b}
Class Name:      <NO CLASS>
Last Write Time: 15-Feb-14 - 9:49 AM
Value 0
  Name:          DeviceInstance
  Type:          REG_SZ
  Data:          USBSTOR
\Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_0.00\12B220719217011A&0
```

Fig. 16 First time after device was connected after last reboot

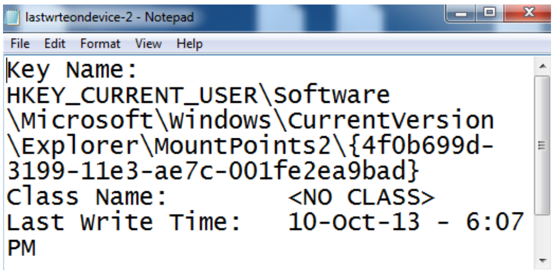
Step 8: Determine the last time device was connected on the basis of serial number.

Case-1: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 {GUIDS}



```
Key Name:
HKEY_CURRENT_USER\Software
\Microsoft\Windows\CurrentVersion
\Explorer\MountPoints2\{4f2a2569-
90c2-11e3-9f6f-001fe2ea9bad}
Class Name:        <NO CLASS>
Last Write Time:   08-Feb-14 - 8:17
PM
```

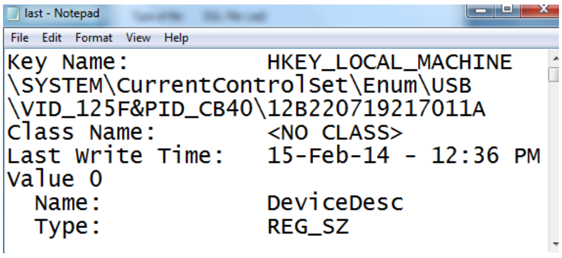
Fig. 17 Last write time on the basis of GUID-1



```
Key Name:
HKEY_CURRENT_USER\Software
\Microsoft\Windows\CurrentVersion
\Explorer\MountPoints2\{4f0b699d-
3199-11e3-ae7c-001fe2ea9bad}
Class Name:        <NO CLASS>
Last Write Time:   10-Oct-13 - 6:07
PM
```

Fig. 18 Last write time on the basis of GUID-2

Case-2: It might happen that data is not obtained from case-1, in that case you can go with case-2.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\VID_125F&PID_CB40\12B220719217011A



```
Key Name:          HKEY_LOCAL_MACHINE
\SYSTEM\CurrentControlSet\Enum\USB
\VID_125F&PID_CB40\12B220719217011A
Class Name:        <NO CLASS>
Last Write Time:   15-Feb-14 - 12:36 PM
Value 0
  Name:            DeviceDesc
  Type:            REG_SZ
```

Fig. 19 Last write time obtained

V. Conclusions and Future Scope

From the above section it can be concluded that the data has been copied into the USB device as the MAC time of the file suspected (customers.sql) of being copied is checked and compared to the time obtained through the registry analysis (see the time obtained in step 8). It was observed from the Modified, Accessed & Created times of the file in the system that, access times of customers.sql is changed and is within the vicinity of the last write time of the device. Hence, it may be concluded that the USB device was connected at that particular time and now the device is in question. The things analyzed so far signifies that file has been copied to the USB disk. The Victim can go with the cyber laws and submit the results obtained by the forensic analysis. The clues can be submitted to the forensic experts and then they can really discover more hidden data by applying forensic analysis on registry, memory, device, computer etc.

The present paper deals the manual investigation process. Here the suspected file customers.sql was made gone though the investigation process. Practically in a system there are many sources of sensitive and critical information that needs to be secured and at times it may be analyzed. Therefore, the present research can be upgraded and new solutions can be identified which will be very helpful in performing forensic analysis easily. Hence, the future scope may contain the following analysis-

i. Forensic Analysis on Windows 8 operating system
ii. 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.
iii. The file was copied because; the USB device plugged can work. One solution can be- disabling the USB ports by changing some registry keys.
iv. A background process can be developed which records the timestamps for the devices being connected to the system. This includes both plug-in time and plug-out time. Later these values can be very helpful in forensic analysis. At present, no system records the plug-out time. It's an important factor which can be very useful while analyzing the PnP (Plug & Play devices).

References

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

[2] 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

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

[4] 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

[5] 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

[6] 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

[7] 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

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

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

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

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

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

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

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

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.