



Windows Forensics

MODULE 7

Contents

7.1 Learning Objectives	3
7.2 Introduction to Windows Forensics	3
7.2.1 Background and need for Window forensics	4
7.2.2 Major forensic areas in windows	5
5.2.2.1 Volatile information	5
7.2.2.2 Non Volatile information	11
7.3 Summary	14
7.4 Check Your Progress	15
7.5 Answers to Check Your Progress	15
7.6 Further Readings	15
7.7 Model Questions	16
References, Article Source & Contributors	16
Bibliography	16

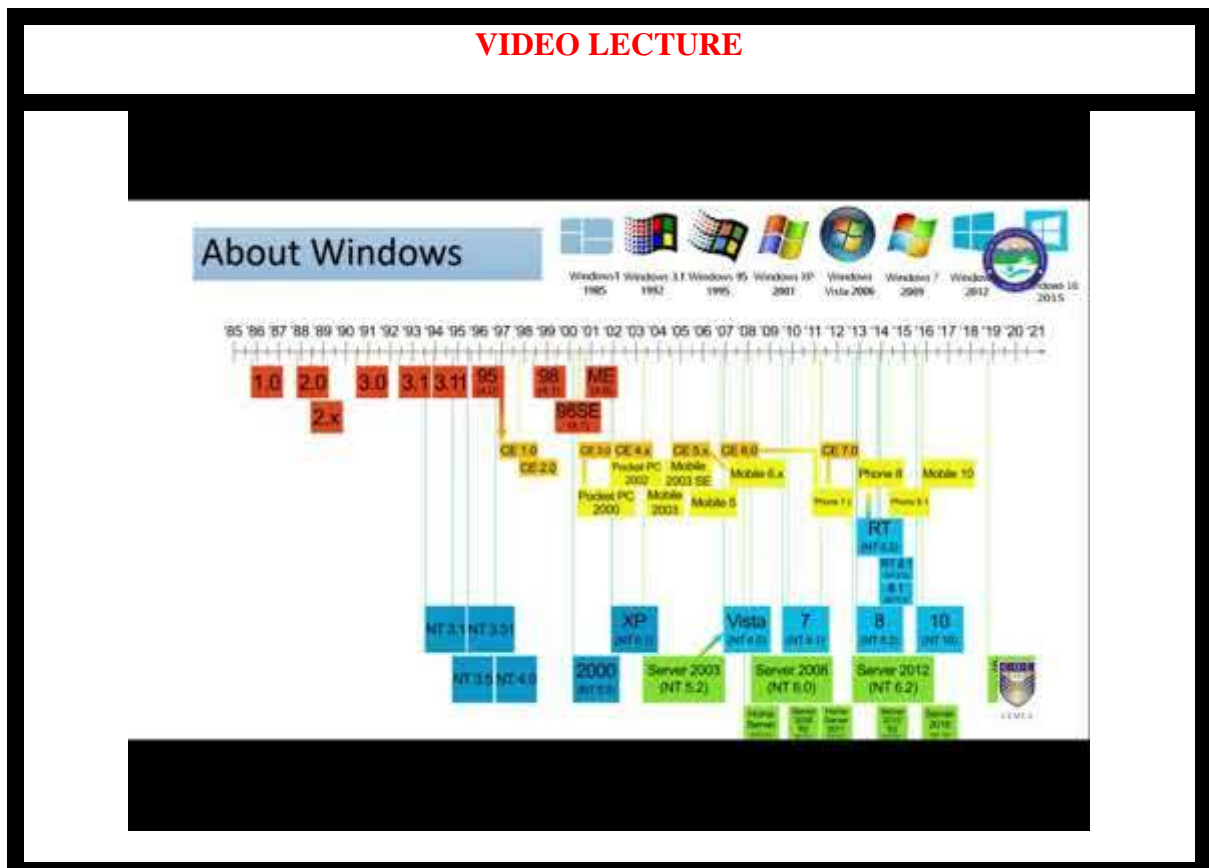
Windows Forensics

7.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Appreciate the need for windows forensics.
- Explain various technical terminologies associated to forensics in windows systems.
- Identify major components and aspects of windows which are relevant during forensics.
- Define basic technologies and tools used to carry out data capture from a windows system during forensic investigation.
- Use basic tools and technologies for capturing registry information from windows systems during forensic investigation.

7.2 INTRODUCTION TO WINDOWS FORENSICS



Computer forensics involves analysis of a computer system and identifies traces or evidences

of activities leading to a criminal activity. In a sense much of the criminal activities in current world have more than one link to computing environments or at least has some or other relation to computers. Most of the criminal/other investigation tends to find traces of data or information in a computer system that can lead to conclusion or at least leads to support a theory pertaining a criminal offence. Windows forensics involves analysing various aspects of windows for malicious or suspicious traces of data in order to reach an evidential conclusion of any case. Windows forensics process is to analyse gathered information from activities that took place in a windows system. Aspects of windows like the registry, files, cookies, bins, memory status etc. contains initial information that can be used to promise a conclusion.

7.2.1 Background and need for Window forensics



Among the major operating system in use, Microsoft window is the most widely used operating system. The Microsoft windows versions that are currently in use are; Windows 8 and Windows 10. Microsoft Windows originated in 1985, as an operating environment running on top of MS DOS, which was the standard operating system shipped on most of Intel architecture PCs.

In 1995, Windows 95 was released which only used MS-DOS as a bootstrap. For backwards compatibility, Win9x could run real-mode MS-DOS and 16 bits Windows3.x drivers. Windows ME, released in 2000, was the last version in the Win9x

family. Later versions have all been based on the Windows NT kernel. Server editions of Windows are widely used. In recent years, Microsoft has expended significant capital in an effort to promote the use of Windows as a server operating system. However, Windows' usage on servers is not as widespread as on personal computers

To know about windows artefacts is quite important for digital forensics examiners, almost 90 percent of traffic in networks comes from computers using Windows as their operating system and the investigators will be most likely to encounter Windows and have to collect evidence from it in most of the cybercrime cases. Below, we will discuss several places from which evidence may be gathered and ways to collect information from Windows.

This chapter focuses on Windows forensics. It starts by covering the different types of volatile and non-volatile information an investigator can collect from a Windows system.

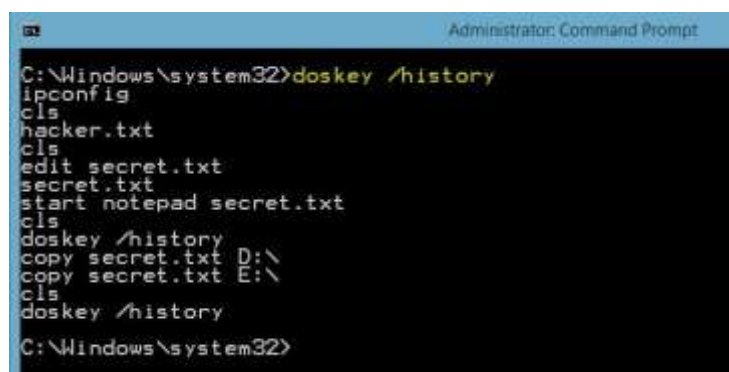
7.2.2 Major forensic areas in windows

More generally an investigator likes to access and analyse following areas in windows:

- a) Volatile information like, system time, logged users, open files, network information and drives that are mapped shared folders etc. These and many more aspects will be discovered in the next section under the windows volatile information head.
- b) Non-volatile information like file systems, registry settings, logs, devices, slack space, swap file, indexes, partitions etc. these and many more will be discovered in coming section under the heading non-volatile information.
- c) Windows memory like memory dumps and analysing dumps and other aspects.
- d) Caches, cookies and history analysis.
- e) Other aspects like recycle bins, documents, short cut files, graphics file, executable files etc.

5.2.2.1 Volatile information

Volatile Information can disappear or be easily modified. It retains its contents while powered on but when the power is interrupted the stored data is immediately lost. Following are few methods/tools to acquire some volatile information in a Windows system. To get history of commands used on the computer we can use Doskey. Doskey is a utility for DOS and Microsoft Windows that adds command history (see figure 2.1).



```
Administrator: Command Prompt
C:\Windows\system32>doskey /history
ipconfig
cls
hacker.txt
cls
edit secret.txt
secret.txt
start notepad secret.txt
cls
doskey /history
copy secret.txt D:\
copy secret.txt E:\
cls
doskey /history
C:\Windows\system32>
```

Figure 1: Doskey utility in Windows command prompt.

To get the current uptime and system events and statistics of the local or remote system we can use a utility called Uptime2.exe. See Figure 2.

```
C:\Windows\System32>Uptime2.exe /s
This utility is developed by Sitaram Pamarthi'(http://techibee.com')
Use /nologo parameter to suppress this banner message

\\WIN-M99E0USEF1H has been up for: 0 days(s), 5 hour(s), 29 minute(s), 57 second
s
Computer startup at: 12/19/2014 11:43:36 AM
Computer shutdown at: 12/19/2014 9:43:03 AM
Computer startup at: 12/18/2014 11:48:44 PM
Computer shutdown at: 12/15/2014 1:42:20 AM
Computer startup at: 12/13/2014 10:31:57 AM
Computer startup at: 12/12/2014 10:35:45 AM
Computer shutdown at: 12/9/2014 7:47:31 PM
Computer startup at: 12/9/2014 3:05:45 PM
Computer startup at: 11/30/2014 10:10:56 AM
Computer shutdown at: 11/29/2014 1:00:33 AM
```

Figure 2: Uptime2.exe output giving uptimes for the windows system.

During an investigation we will always need to know who all were logged on to the system. Logging to a system can be remotely or locally. Information like these can add logical view to a context or a situation. The logs can be related to an event occurrence. Many tools are available like PsLoggedon, Netsessions, logonsessions etc. to learn the instantaneous information of the users. These tools can be downloaded from the windows sysinternals site. Ps tools in sysinternals are handy in many ways as such. See figure 3,4,5.

VIDEO LECTURE

Tlist, Tasklist, Pslist, ListDlls

```

C:\Users\user\Desktop\data>sysinternals>pslist
pslist v1.3 - Sysinternals PsList
Copyright (C) 2000-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for IT385-681:

Name           Pid  Pri  Thr  Mem  Priu      CPU Time  Elapsed Time
-----
Idle            0     0    4    0     0      5:32:51.015  1:30:48.553
System         4     8  112 1024    196      0:00:00.265  1:30:48.553
smss          364    11   7   44     275      0:00:01.937  1:30:48.476
svchost       464    13  10  381    2356     0:00:01.875  1:30:36.443
smss          544    13  12  335    2436     0:00:00.593  1:30:32.227
smss          562    13   1    76     292     0:00:00.500  1:30:32.227
svchost       600    13   2   176    1532     0:00:00.561  1:30:31.587
svchost       640    7   4  290    4356     0:00:05.898  1:30:24.584
svchost       648    7   8 1100    5676     0:00:03.875  1:30:24.423
svchost       724    8   9  510    5852     0:00:01.265  1:30:20.006
svchost       768    8   7  487    4472     0:00:01.312  1:30:17.096
lsass         800    13   6  196    18236     0:00:54.214  1:30:19.709
svchost       872    8  36  641 113148     0:02:59.156  1:30:19.631
svchost       964    8   5  109    876     0:00:00.000  1:30:17.165
svchost       988    8  23  762  16440     0:00:03.625  1:30:17.210
svchost       80    8  39 2738  31640     0:00:16.593  1:30:17.146
svchost       444    8  20  582   8548     0:00:00.640  1:30:16.974
svchost       420    8  11  424  97992     0:02:16.984  1:30:16.660
svchost       1044   8  39  906 104008     0:00:01.312  1:30:16.240
svchost       1224   8  13  448   5600     0:00:00.934  1:30:16.004
svchost       1348   8  25  473  23326     0:00:01.795  1:30:16.060
svchost       1400   8  60  408  26100     0:00:00.250  1:30:14.519
svchost       1468   8  10  363   4664     0:00:00.203  1:30:11.666
smss          1512   8  21  240   4120     0:00:00.011  1:30:11.541

```



```

C:\WINDOWS\system32\cmd.exe

C:\>openfiles

INFO: The system global flag 'maintain objects list' needs to be enabled to see
local opened files. See Openfiles /? for more information.

Files Opened Remotely via local share points:
-----
ID           Accessed By      Type      Open File (Path\executable)
-----
33          MOHAMMADHD      Windows   D:\SHARE
111         MOHAMMADHD      Windows   D:\SHARE\cpuspeed.exe

C:\>

```

Figure 6: openfiles output.

Tools like NetStat gives access to information partitioning current network connections to the host computer. This information will be lost over time and very difficult to trace as time passes by. Figure 7 gives an output of the NetStat command. Also, an investigator needs to discover what processes are running on the system. This system which can keep clues to a major crime in form of files or processes that are still on the acquired system is potentially used just before a crime. Information about processes like executable file path, commands to launch the process, time stamps, current modules etc. along with contexts needs to be collected. Tools like Tlist, Tasklist, Pslist, ListDlls etc. helps us to get all these information. Windows task manager does give some information but most of the time it does not show vital information, hence using above tools play significant role in forensics.

```

c:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\admin>netstat

Active Connections

Proto Local Address          Foreign Address        State
TCP   admin:2231             xxx.xxx.hr:pop3        TIME_WAIT
TCP   admin:2232             xxx.xxx.hr:pop3        TIME_WAIT
TCP   admin:2233             xxx.xxx.com:pop3       TIME_WAIT

C:\Documents and Settings\admin>netstat -n

Active Connections

Proto Local Address          Foreign Address        State
TCP   192.168.1.2:2231       xxx.xxx.142.116:110    TIME_WAIT
TCP   192.168.1.2:2232       xxx.xxx.150.5:110     TIME_WAIT
TCP   192.168.1.2:2233       xxx.xxx.100.127:110   TIME_WAIT

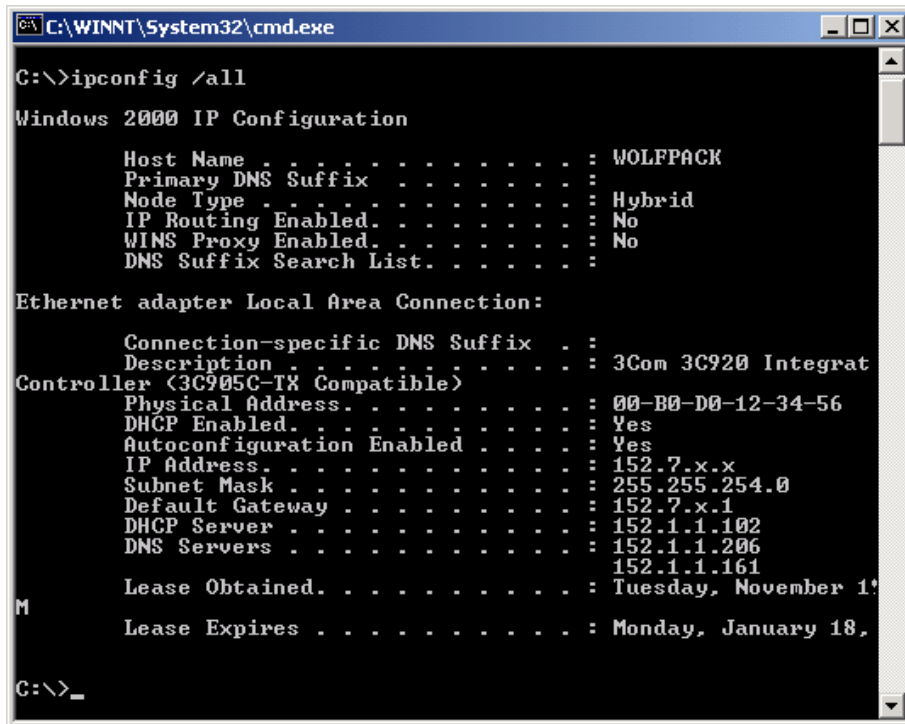
C:\Documents and Settings\admin>

```

Figure 7: NetStat output.

Information about the status of the network interface cards (NIC) connected to a system can be very important. Wireless interfaces are very prominent these days and physical connection does not have too much presence. Hence, it's important to know the status of all interface devices (Network) is important. Tools like ipConfig, promiscDetect, promgry helps in getting the vital

information (see Figure 8, Figure 9, Figure 10). Clipboards of windows are another aspect which is of utmost importance to the investigators. Clipboards contain latest copied area of memory which can be for later use. Clipboards facilitate users to move data in some way between documents or applications. The fact that recently copied and pasted items do remain on clipboard can give clue to vital evidences or circumstances leading to a crime. pclip is a command-line utility which helps the investigators to retrieve contents of a clipboard.



```
C:\WINNT\System32\cmd.exe
C:\>ipconfig /all

Windows 2000 IP Configuration

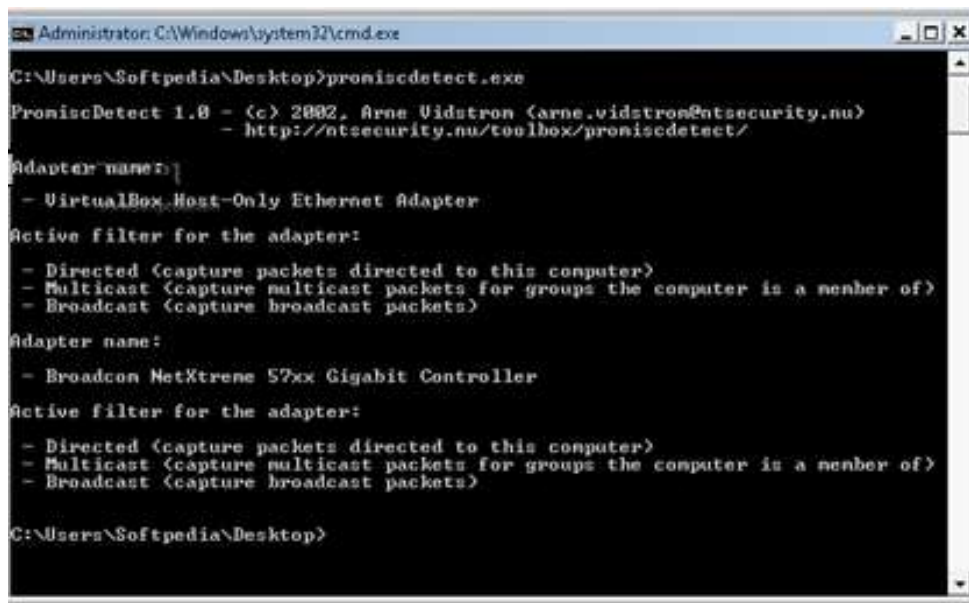
    Host Name . . . . . : WOLFPACK
    Primary DNS Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . :

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . :
    Description . . . . . : 3Com 3C920 Integrat
Controller (3C905C-TX Compatible)
    Physical Address. . . . . : 00-B0-D0-12-34-56
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 152.7.x.x
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 152.7.x.1
    DHCP Server . . . . . : 152.1.1.102
    DNS Servers . . . . . : 152.1.1.206
    . . . . . : 152.1.1.161
    Lease Obtained. . . . . : Tuesday, November 19, 2002 10:00:00 AM
    Lease Expires . . . . . : Monday, January 18, 2003 10:00:00 AM

C:\>_
```

Figure 8: one of the output of ipConfig command.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Softpedia\Desktop>promiscdetect.exe
PromiscDetect 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- http://ntsecurity.nu/toolbox/promiscdetect/

Adapter name:
- VirtualBox Host-Only Ethernet Adapter
Active filter for the adapter:
- Directed (capture packets directed to this computer)
- Multicast (capture multicast packets for groups the computer is a member of)
- Broadcast (capture broadcast packets)

Adapter name:
- Broadcom NetXtreme 57xx Gigabit Controller
Active filter for the adapter:
- Directed (capture packets directed to this computer)
- Multicast (capture multicast packets for groups the computer is a member of)
- Broadcast (capture broadcast packets)

C:\Users\Softpedia\Desktop>
```

Figure 9: Promiscdetect command.

```

Administrator: C:\Windows\system32\cmd.exe
SOFTPEDIA

Querying local system...

Active: True
InstanceName:
Microsoft ISATAP Adapter
NEGATIVE: Promiscuous node currently NOT enabled

Active: True
InstanceName:
Teredo Tunneling Pseudo-Interface
NEGATIVE: Promiscuous node currently NOT enabled

Active: True
InstanceName:
Realtek PCIe GBE Family Controller
POSITIVE: Promiscuous node enabled!

Active: True
InstanceName:
WAN Miniport (Network Monitor)
NEGATIVE: Promiscuous node currently NOT enabled

Active: True
InstanceName:
WAN Miniport (IP)
NEGATIVE: Promiscuous node currently NOT enabled

Active: True
InstanceName:
WAN Miniport (IPv6)
NEGATIVE: Promiscuous node currently NOT enabled

Active: True
InstanceName:
RAS Async Adapter
NEGATIVE: Promiscuous node currently NOT enabled

System Summary
POSITIVE: at least one interface on system was found in promiscuous mode.

Computer name: SOFTPEDIA-OLI
Domain: SOFTPEDIA
Computer manufacturer: Dell Inc.
Computer model: OptiPlex 390
Primary owner: Softpedia
User currently logged on: SOFTPEDIA-OLI\Softpedia
Operating system: Microsoft Windows 7 Professional
Organization:

*****

```

Figure 10: Promqry Command output.

```

C:\wpromqry>promqry /?

Promqry version 1.0 usage

Queries system(s) for interfaces
running in promiscuous mode

To query local system's interfaces run:

    promqry.exe

notes: returns zero if any interfaces found in promiscuous mode
       returns 1 if no interfaces found in promiscuous mode
       returns 99 if error encountered
       -np and -nv options are not valid for local query

To query a remote system's interfaces run:

    promqry.exe remote_IP ! remote_name [-nv]

notes: returns zero if any interfaces found in promiscuous mode
       returns 1 if no interfaces found in promiscuous mode
       returns 99 if error encountered
       -nv means no verbose output, only reports errors and
           systems with interfaces in promiscuous mode

To query a range of remote systems' interfaces run:

    promqry.exe start_remote_IP:end_remote_IP [-np] [-nv]

notes: start_remote_IP must be lower than end_remote_IP
       -np means no ping before query
       -np only valid when querying range of systems
       -nv means no verbose output, only reports errors and
           systems with interfaces in promiscuous mode

```

Figure 11: various options with promqry.

Several other information like; mapped drives, shares or stored folders etc. also needs to be collected for future tests and analysis. Mapped drives to a system are those which the user has created. These information are volatile but can be correlated to network connections or drive activities leading to a crime. A system resources can be shared in many different ways like shared folders, shared network access etc. This information can be retrieved in many ways like scanning the registry for shares. Also, command like 'share' can be used for the same.

7.2.2.2 Non Volatile information

Non-volatile information remains on a secondary storage device and persists even after power is off. This information can be collected later on after all perishable information (volatile) can be collected after the seizure of the system. Investigators can collect these information after procuring the device and doing all the formalities of the seizure/procuring/capturing the device under law so that the discoveries later on does not get laid down during hearing. Using command line 'dir /o: d' the examiner can list out the recent updates that is listed by the command.



Registry information

Registry information can have a good impact on the forensic analysis and investigation. Tools like *reg* (see figure12,13) and *regedit* (see figure 14) helps in to get registry entries via important keys. Few important keys present in registries are runMRU, startup

objects, last accessed key, addresses in internet explorer, last saved directory in internet explorer.

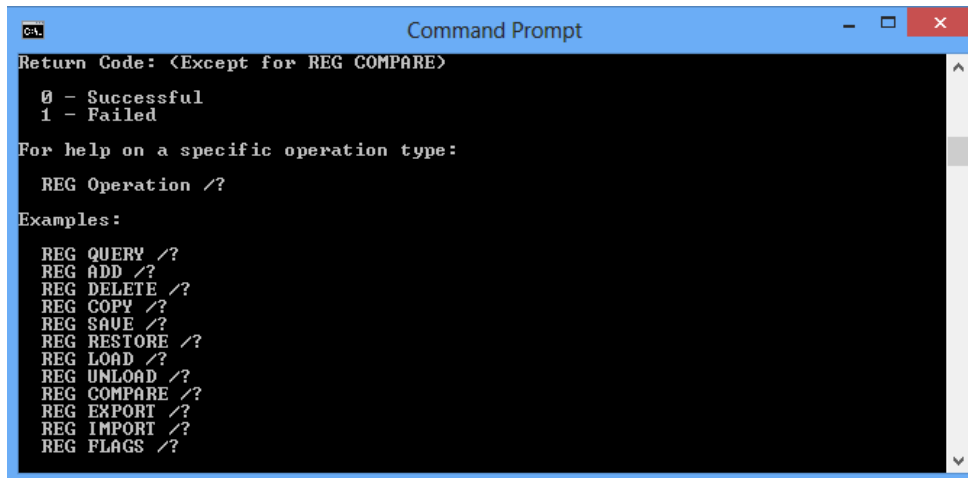


Figure 12: Options in reg tool.

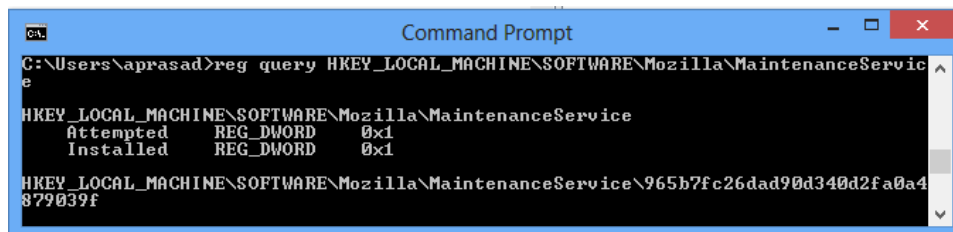


Figure 13: example output of reg.

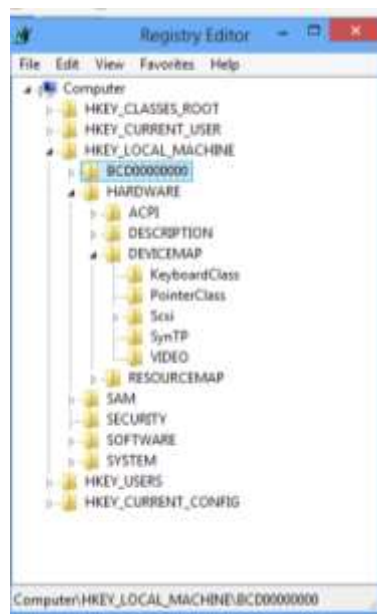


Figure 14: regedit command in windows.

RunMRU stores information about recently typed commands from run window, startup objects are those objects or apps that start automatically on startup in windows.

Key for RunMRU is:

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

Key for startup object is:

Computer\HKCU\<SID>\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Computer\HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

To access the least accessed key in registry use key:

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit

To get last typed urls in internet explorer use key:

Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedUrls

To get last saved directory in IE use key:

Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer Download Directory

To get security ids Microsoft use:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList key

Another area of registry which has valuable information for forensics analysis is the protected storage area. These storages are encrypted. However, we can get access to these areas using tools like *Access Data tool kit* (see figure 15).

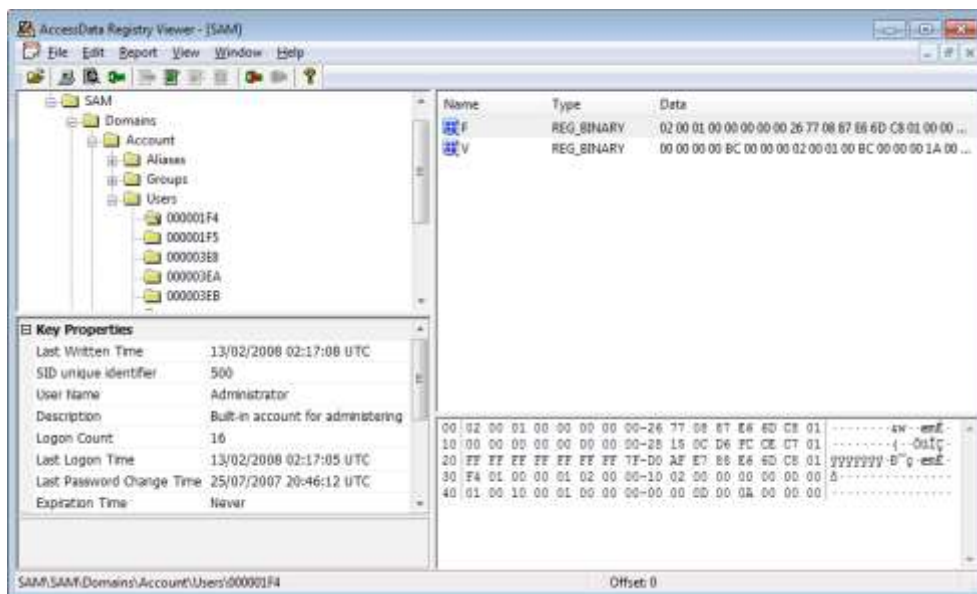
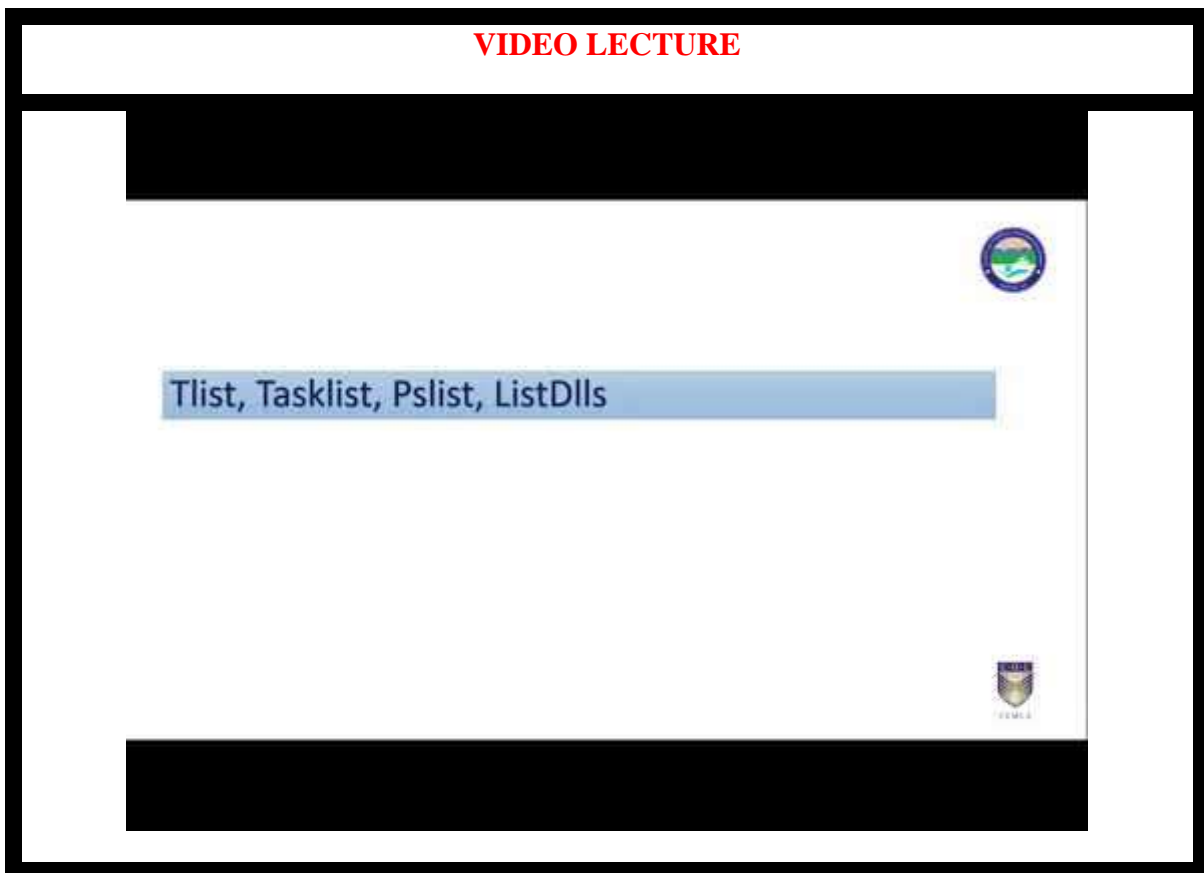


Figure 15: AccessData tool window.

Some time it may be very important to get record what are all the devices that were connected to a system. To gain access to this information we can use tools like (windows device console) *DevCon* of Microsoft. Device manager of windows is also available for some Figure 16 shows the output of *DevCon*.

```
C:\WINDOWS\system32\cmd.exe
updateini Manually update a device (non interactive).
C:\SVSetup\devcon\i386>devcon huids: "pci\ven_8086&dev_27dc"
PCI\VEN_8086&DEV_27DC&SUBSYS_336C1462&REV_01\481AF1648C&0840F0
Name: Ethernet Controller
Hardware ID's:
PCI\VEN_8086&DEV_27DC&SUBSYS_336C1462&REV_01
PCI\VEN_8086&DEV_27DC&SUBSYS_336C1462
PCI\VEN_8086&DEV_27DC&CC_020000
PCI\VEN_8086&DEV_27DC&CC_0200
Compatible ID's:
PCI\VEN_8086&DEV_27DC&REV_01
PCI\VEN_8086&DEV_27DC
PCI\VEN_8086&CC_020000
PCI\VEN_8086&CC_0200
PCI\VEN_8086
PCI\CC_020000
PCI\CC_0200
1 matching device(s) found.
```

Figure 16: Devcon output.



indow (showing system).

7.3 SUMMARY

1. Registry information can have a good impact on the forensic analysis and investigation and collecting these information would be very vital.
2. Tools like *DevCon*, *Access Data tool kit*, *reg* and *regedit* helps in extracting non-volatile information in Windows.
3. Windows organises data using structures or elements like *Cluster*, *Partition*, *Master Boot Record*, *FAT32*, *New Technology File System*.

4. Files that are deleted, lost, cached or unallocated can be retrieved using various methods and tools.

7.4 CHECK YOUR PROGRESS

1. Fill in the blanks.

- a) _____ in windows contain latest copied area of memory which can be for later use.
- b) Tools like *reg* and *regedit* helps in to get _____ via important keys.
- c) In computer disk storage, a _____ is a subdivision of a track on a magnetic disk or optical disc.
- d) _____ is the amount of on-disk file space from the end of the logical record information to the end of the physical disk record.
- e) _____ is the process of trying to recover files without a file system metadata.

2. State True or False.

- a) Registry information is an example of volatile information
- b) Group of sectors form a cluster.
- c) When a file is deleted, the file system removes the file logically i.e. it removes all the meta-data and stamps related to the file.

7.5 ANSWERS TO CHECK YOUR PROGRESS

1. Fill in the blanks.

- a) Clipboards.
- b) Registry entries.
- c) Sector.
- d) Slack space.
- e) File carving.

2. State True or False

- a) (F)
- b) (T)
- c) (T)

7.6 FURTHER READINGS

- Windows Forensic Analysis Toolkit, Third Edition: Advanced Analysis Techniques for Windows 73rd Edition, by Harlan Carvey.
- File system forensic analysis 1st edition, by Brian carrier
- <http://www.gfi.com/blog/top-20-free-digital-forensic-investigation-tools-for-sysadmins/>
- Linda Volonino, Reynaldo Anzaldua; Computer Forensics For Dummies, Wiley Publishing, Inc.

- Investigating Hard Disks, File and Operating Systems: EC-Council | Press

7.7 MODEL QUESTIONS

1. Describe the disk and file structure in a windows system.
2. What is a slack space, swap space and file carving?
3. How is registry information important in windows forensics?

References, Article Source & Contributors

- [1] Disk Sector, https://en.wikipedia.org/wiki/Disk_sector, retrieved Nov 2015
- [2] DriveSpy, <https://www.digitalintelligence.com/software/disoftware/drivespy/>, retrieved Nov 2015
- [3] File Carving, https://en.wikipedia.org/wiki/File_carving, retrieved Nov 2015
- [4] Hard Disk Drive, https://en.wikipedia.org/wiki/Hard_disk_drive, retrieved Nov 2015
- [5] Operating Systems, https://en.wikipedia.org/wiki/Operating_system, retrieved Nov 2015
- [6] What is slack space, A Webopedia Definition, www.webopedia.com/TERM/S/slack_space

Bibliography

- [1] Windows System artefacts, <http://resources.infosecinstitute.com/windows-systems-and-artifacts-in-digital-forensics-part-i-registry/>, retrieved Nov 2015
- [2] Tom Olzak, IT Security, <http://www.techrepublic.com/blog/it-security/computer-forensics-finding-hidden-data/>, May 21, 2007, retrieved Nov 2015.

RECOMMENDED YOUTUBE LECTURE

1. Introduction to Windows Forensics: <https://youtu.be/VYROU-ZwZX8>

EXPERT PANEL



**Dr. Jeetendra Pande, Associate Professor- Computer Science, School of
Computer Science & IT, Uttarakhand Open University, Haldwani**



**Dr. Ajay Prasad, Sr. Associate Professor, University of Petroleum and
Energy Studies, Dehradun**



**Dr. Akashdeep Bharadwaj, Professor, University of Petroleum and Energy
Studies, Dehradun**



**Mr. Sridhar Chandramohan Iyer, Assistant Professor- Universal College of
Engineering, Kaman, Vasai, University of Mumbai**



Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert



Ms. Priyanka Tewari, IT Consultant



Mr. Ketan Joglekar, Assistant Professor, GJ College, Maharashtra



Dr. Ashutosh Kumar Bhatt, Associate Professor, Uttarakhand Open University, Haldwani



Dr. Sangram Panigrahi, Assistant Professor, Siksha 'O' Anusandhan, Bhubaneswar



This MOOC has been prepared with the support of



© Commonwealth Educational Media Centre for Asia , 2021. Available in Creative Commons Attribution-ShareAlike 4.0 International license to copy, remix and redistribute with attribution to the original source (copyright holder), and the derivative is also shared with similar license.