

Operating System Forensics

Module 06



Operating System Forensics

Module 06

Designed by **Cyber Crime Investigators**. Presented by Professionals.




Computer Hacking Forensic Investigator v9

Module 06: Operating System Forensics

Exam 312-49

Module Objectives



→ After successfully completing this module, you will be able to:

- 1 Understand how to collect and examine volatile and non-volatile data in Windows machines
- 2 Perform windows memory and registry analysis
- 3 Examine the cache, cookie, and history recorded in web browsers
- 4 Examine Windows files and metadata
- 5 Analyze text based logs and Windows event logs
- 6 List various Linux based shell commands and log files
- 7 Collect and examine volatile and non-volatile information in Linux machines
- 8 Explain the need for Mac forensics and examine Mac forensics data and log files

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

“Operating System Forensics” refers to the process of finding, extracting and analyzing evidences present in the operating system of any computerized device used by the victim, or suspected computer system involved in any security incident. Most commonly used operating systems include Microsoft Windows, Linux, and MAC. They are often the most common target and source of criminal activities.

Forensic investigators should possess a complete understanding of these operating systems, along with detailed knowledge of their *modus operandi*. This module will discuss the topics mentioned in the slide represented above.

Introduction to OS Forensics





Windows Mac Linux Most commonly used operating systems that you may face these

OS Forensics to **uncover the underlying evidence** is slightly different from a traditional investigator as they were not specifically designed for this purpose.





To conduct a successful **digital forensic examination** in Windows, Mac, and Linux, one should be **familiar with** their **working, commands** or **methodologies**, which meant to extract volatile and non-volatile data, OS specific tools, etc.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

“OS Forensics” involves forensic examination of the operating system of the computer. The most commonly used operating systems are Windows, Mac, and Linux. It is highly likely that the forensic investigators may come across one of these operating systems during any crime investigation. It is imperative that they have thorough knowledge about these operating systems, their features, methods of processing, data storage and retrieval as well as other characteristics.

The investigators should also have in depth understanding of the commands or methodologies used, key technical concepts, process of collecting volatile and non-volatile data, memory analysis, Windows registry analysis, cache, cookie, and history analysis, etc. in order to conduct a successful digital forensic investigation.

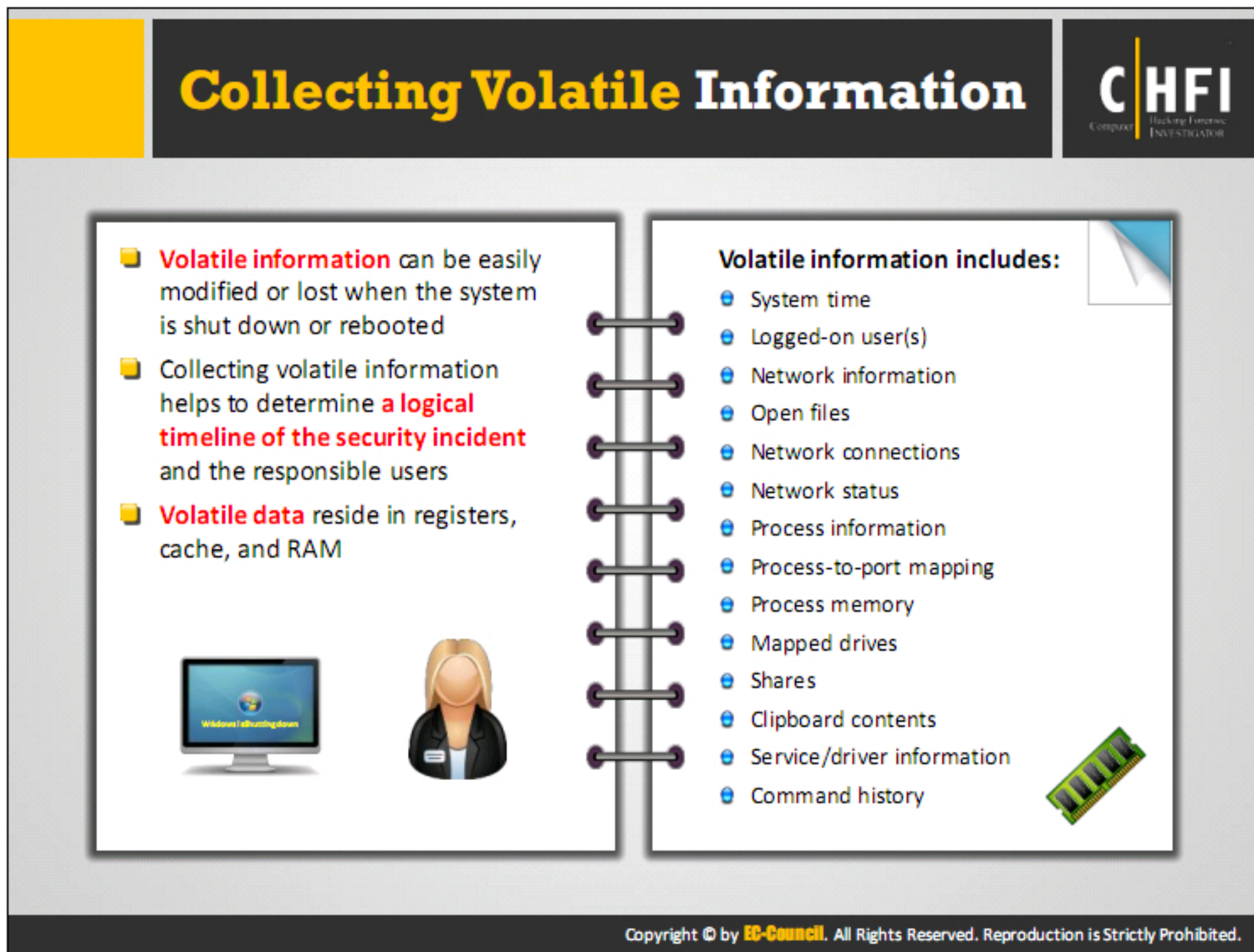


Windows Forensics, include the process of conducting or performing forensic investigations of systems which run on Windows operating systems. It includes analysis of incident response, recovery, and auditing of equipment used in executing any criminal activity. In order to accomplish such intricate forensic analyses, the investigators should possess extensive knowledge of the Microsoft Windows operating systems.

This module will discuss about collecting volatile and non-volatile information; performing windows memory and registry analysis; cache, cookie, and history analysis; MD5 calculation, windows file analysis, etc.



Most of the systems store data related to the current session in temporary form across registries, cache, and RAM. This data is easily lost when the user switches the system off, resulting in loss of the session information. Therefore, the investigators need to extract it as a priority. This section will help you understand the volatile data, its importance and ways to extract it.




Volatile Information refers to the data stored in the registries, cache, and RAM of digital devices. This information is usually lost or erased whenever the system is turned off or rebooted. The volatile information is dynamic in nature and keeps on changing with time; so the investigators should be able to collect the data in real time.

Volatile data exists in physical memory or RAM and consists of process information, process-to-port mapping, process memory, network connections, clipboard contents, state of the system, etc. The investigators must collect this data during the live data acquisition process.

The investigators follow the Locard's Exchange Principle and collect the contents of the RAM right at the onset of investigation, so as to minimize the impact of further steps on the integrity of the contents of the RAM. Investigators are well aware of the fact that the tools they are running to collect other volatile information cause modification of the contents of the memory. Based upon the collected volatile information, the investigators can determine the user logged on, timeline of the security incident, programs and libraries involved, files accessed and shared during the suspected attack, as well as other details.

System Time



- Provides details of the **information collected** during the **investigation**
- It helps in re-creating the **accurate timeline** of events that occurred on the system
- System uptime provides an idea of when an **exploit attempt** might have been successful

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Admin>date /t & time /t
Thu 04/14/2016
10:57 AM
C:\Users\Admin>
```

```
C:\WINDOWS\system32\cmd.exe
C:\Users\Admin>net statistics server
Server Statistics for \RD-006

Statistics since 3/10/2016 3:32:50 AM

Sessions accepted                0
Sessions timed-out               0
Sessions errored-out             1
Kilobytes sent                   21244
Kilobytes received               3880
Mean response time (nsec)       0
System errors                   0
Permission violations            0
Password violations              5
Files accessed                   1875
Communication devices accessed  0
Print jobs spooled               0
Times buffers exhausted

  Big buffers                    0
  Request buffers                0

The command completed successfully.

C:\Users\Admin>
```

Note: Acquire or duplicate the memory of the target system before extracting volatile data, as the commands used in the process can alter contents of media and make the proof legally invalid

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


The first step while investigating an incident is the collection of the system time. System time refers to the exact date and time of the day when the incident happened, as per the coordinated universal time (UTC). The system provides the system time so that the applications launched have access to the accurate time and date.

The knowledge of system time will give a great deal of context to the information collected in the subsequent steps. It will also assist in developing an accurate timeline of events that have occurred on the system. Apart from the current system time, information about the amount of time that the system has been running, or the uptime, can also provide a great deal of context to the investigation process.

Investigators also record the real time, or wall time, when recording the system time. Comparison of both the timings allows the investigator to further determine whether the system clock was accurate or inaccurate. The investigators can extract system time and date with the help of the `date /t & time /t` command or use the `net statistics server` command.

An alternative way for obtaining the system time details is by using the `GetSystemTime` function. This function copies the time details to a `SYSTEMTIME` structure that contains information of individual logged in members and the exact information of month, day, year, weekday, hour, minute, second, and milliseconds. Hence, this function provides better accuracy to the system time details.

Logged-On Users



I


Collect the information about **users logged on to the system**, both locally and remotely

II

Note down complete details of a **running process**, the owner of a file, or the last access time on files

Tools and commands to determine logged-on-users

- PsLoggedOn
- net sessions
- LogonSessions



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

During an investigation, an investigator must gather details of all the users logged on to the suspected system. This not only includes the information of people logged on locally (via the console or keyboard) but also those who had remote access to the system (e.g. - via the net use command or via a mapped share). This information allows an investigator to add context to other information collected from the system, such as the user context of a running process, the owner of a file, or the last access times on files. It is also useful to correlate the collected system time information with the Security event log, particularly if the admin has enabled appropriate auditing.

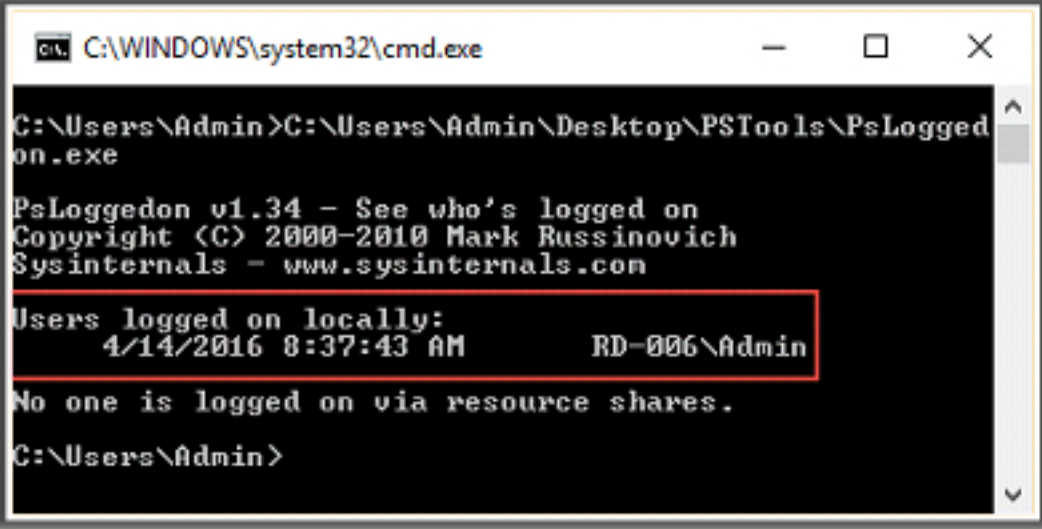
Some of the tools and commands used to determine logged-on users are as follows:

- PsLoggedOn
- net sessions
- LogonSessions

Logged-On Users: PsLoggedOn Tool



- PsLoggedOn is an applet that **displays** both the **users logged on** locally and via resources for either on the local, or a remote computer
- Syntax: **psloggedon [-] [-l] [-x] [\\computername | username]**



```
C:\WINDOWS\system32\cmd.exe

C:\Users\Admin>C:\Users\Admin\Desktop\PSTools\PsLoggedOn.exe

PsLoggedon v1.34 - See who's logged on
Copyright (C) 2000-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
4/14/2016 8:37:43 AM      RD-006\Admin

No one is logged on via resource shares.

C:\Users\Admin>
```

<https://technet.microsoft.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

PsLoggedOn is an applet that displays both the locally logged on users and users logged on via resources for either the local computer, or a remote one. If you specify a user name instead of a computer, PsLoggedOn searches the computers in the network neighborhood and tells you if the user is currently logged on.


Syntax: psloggedon [-] [-l] [-x] [\\computername | username]

-	Shows the options and the measurement units for output values.
-l	Displays only local logons
-x	Does not display logon times.
\\computername	System name for which logon information should be shown
username	Searches the network for those systems to which that user is logged on.

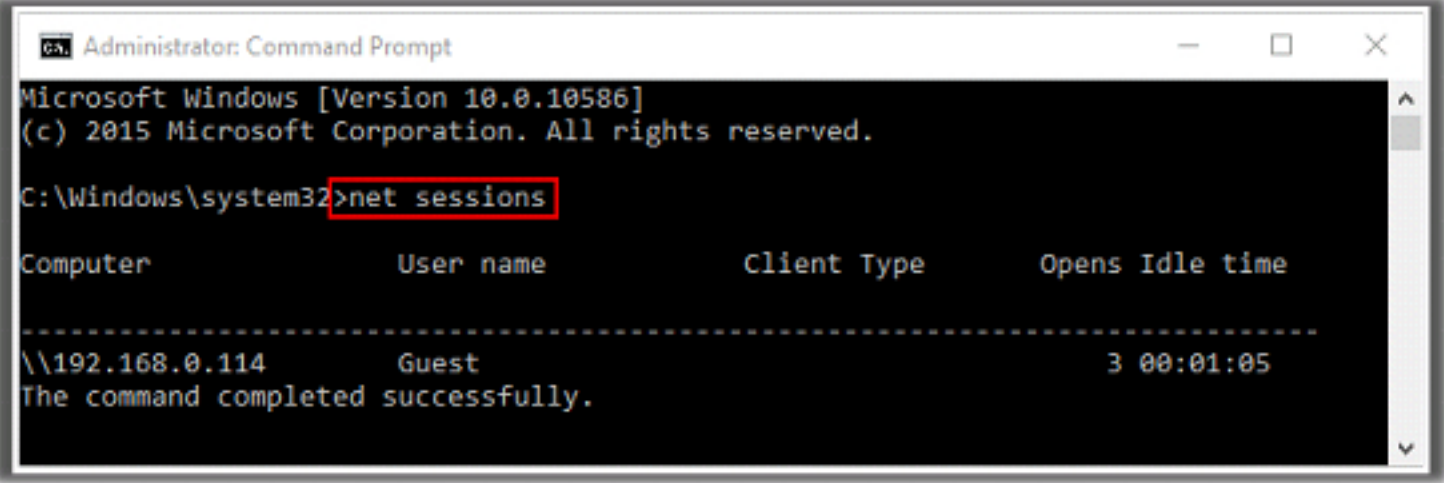
TABLE 6.1: psloggedon parameters

Source: <http://technet.microsoft.com>

Logged-On Users: net sessions Command



- Manages **server computer connections**. Used without parameters, net session displays information about all sessions with the local computer
- It allows to view the **computer names** and **user names** on a server, to see if users have **files open**, and for how long each **user's session has been idle**



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net sessions

Computer          User name          Client Type        Opens Idle time
-----
\\192.168.0.114    Guest              3 00:01:05
The command completed successfully.
```

<https://technet.microsoft.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The net sessions Command is used for managing server computer connections. It is used without parameters and it displays information about all logged in sessions of the local computer. By using this command, one can view the computer names and user names on a server. It can also help us to see if users have any open files and how long each user's session has been in the idle mode.

Syntax: net session [\\ComputerName] [/delete]


\\ComputerName: Identifies the computer for which you want to list or disconnect sessions.

/delete: Ends the computer's session with ComputerName and closes all open files on the computer for the session.


net help command: Displays help for the specified net command.

Source: <http://technet.microsoft.com>

Logged-On Users: LogonSessions Tool



It lists the **currently active logon sessions** and, if the **-p option** is specified, the **processes running in each session**



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32-C:\Users\Admin\Desktop\logonsessions\logonsessions.exe

Logonsessions v1.3
Copyright (C) 2004-2015 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
User name: WORKGROUP\RD-006$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 3/10/2016 3:32:46 AM
Logon server:
DNS Domain:
UPN:

[1] Logon session 00000000:00000209:
User name:
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: (none)
Logon time: 3/10/2016 3:32:46 AM
Logon server:
DNS Domain:
UPN:

[2] Logon session 00000000:000003e4:
User name: WORKGROUP\RD-006$
Auth package: Negotiate
Logon type: Service
Session: 0
Sid: S-1-5-20
Logon time: 3/10/2016 3:32:46 AM
Logon server:
DNS Domain:
UPN:
```

<https://technet.microsoft.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

It lists the currently active logged-on sessions and, if you specify the -p option, it can provide you the information of processes running in each session.


Syntax: logonsessions [-c[t]] [-p]

-c	Prints output as CSV
-ct	Prints output as tab-delimited values
-p	Lists processes running in logged-on sessions

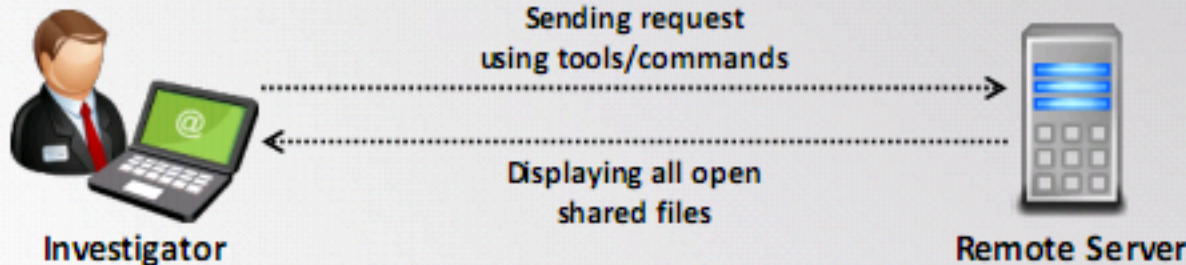
TABLE 6.2: logonsessions parameters

Source: <http://technet.microsoft.com>

Open Files



- Collect the **information about the files opened** by the intruder using remote login
- Tools and commands** used:
 - net file** command
 - PsFile** utility
 - Openfiles** command



```
graph LR; Investigator[Investigator] -- "Sending request using tools/commands" --> RemoteServer[Remote Server]; RemoteServer -- "Displaying all open shared files" --> Investigator;
```

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

When the output obtained from psloggedon.exe commands shows the investigators that there are users logged on to the system remotely, then the investigators will also want to see what files have they opened, if any. Many times when someone accesses a system remotely, they might be looking for something specific while opening files.

A user in a corporate environment could have shared available content and allowed other users to view images, download songs, etc. Anyone can easily gain access to poorly protected systems connected to the internet, with no administrator password (and no firewall), and search for files, and may access and copy them. Tools and commands that show files opened remotely on a system include net file command, psfile.exe, and openfiles.exe.

Open Files: **net file** Command

net file Command**PsFile Utility****Openfiles Command**

- Displays **details of open shared files on a server**, such as a name, ID, and the number of each file locks, if any. It also closes individually shared files and removes file locks
- The syntax of the net file command: **net file [ID [/close]]**



ID	Path	User name	# Locks
252	E:\Finance\	Admin	0
269	C:\Users\Public	Admin	0
315	C:\Users\Public\Pictures	Admin	0
329	E:\Finance\	Admin	0

The command completed successfully.

<https://technet.microsoft.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The net file command displays the names of all open shared files on a server and the number of file locks, if any, on each file. This command can also close individual shared files and remove file locks. When used without parameters, the tool will also display and help to control files shared on the network.

Syntax:

net file [ID [/close]]

- **ID:** Specifies the identification number of the file.
- **/close:** Closes an open file and releases locked records.
- **net help command:** Displays help for the specified net command.

Source: <http://technet.microsoft.com>

Open Files: PsFile Utility



net file Command

PsFile Utility

Openfiles Command

- Command-line utility **shows a list of remotely opened files** on a system as well as allows user to close the opened file either by name or by a file identifier (ID)
- Syntax: **psfile** [\\RemoteComputer [-u Username [-p Password]]] [[Id | path] [-c]]




<https://technet.microsoft.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

PsFile is a command-line utility that can retrieve the list of remotely opened files on a system. It also allows the investigator to close the opened files either by name or by a file identifier. The default behavior of PsFile is to list the files on the local system that are open by remote systems. By typing a command followed by "-" displays information on the syntax for the command.

Syntax: psfile [\\RemoteComputer [-u Username [-p Password]]] [[Id | path] [-c]]

-u	Specifies optional user name for login to remote computer
-p	Specifies password for user name
Id	Identifier (as assigned by PsFile) of the file for which to display information or to close.
Path	Full or partial path of files to match for information display or close.
-c	Closes the files identified by ID or path.

TABLE 6.3: psfile parameters

Source: <http://technet.microsoft.com>

Open Files: Openfiles Command

net file Command

PsFile Utility

Openfiles Command

openfiles /query command output:



Examples:

```
openfiles /disconnect
openfiles /query
openfiles /local
```

<https://technet.microsoft.com>


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Syntax: openfiles.exe /disconnect [/s Computer [/p Password]] [/u Domain\User {[/id OpenFileID] [/a UserName] [/o OpenMode]} [/se SessionName] [/op OpenFileName]

- **/s Computer:** Specifies the name or IP address of a remote computer.
- **/u Domain \ User:** Runs the command with the account permissions of the user specified by User or Domain\User.
- **/p Password:** Specifies the password of the user account that is specified in the /u parameter.
- **/id OpenFileID:** Disconnects the file opened with the specified numeric OpenFileID on the computer specified by the /s parameter.
- **/a UserName:** Disconnects all open files that were accessed by the specified user on the computer specified by the /s parameter.
- **/o OpenMode:** Disconnects all open files with the specified OpenMode on the computer specified by the /s parameter.
- **/se SessionName:** Disconnects all open files that were created by the specified session on the computer specified by the /s parameter.
- **/op OpenFileName:** Disconnects the open file that was created with the specified OpenFileName on the computer specified by the /s parameter.
- **/?:** Displays help at the command prompt.

Source: <http://technet.microsoft.com>

Network Information



- Intruders after gaining access to a remote system, try to discover other systems that are available on the network
- When other systems connect using **NetBIOS**, the system will list all the other visible systems
- NetBIOS name table cache **maintains a list of connections** made to other systems using NetBIOS
- The Windows inbuilt command line utility **nbtstat** can be used to view NetBIOS name table cache
- The **nbtstat -c** option shows the contents of the NetBIOS name cache, which contains NetBIOS name-to-IP address mappings

```
Administrator: Command Prompt
-s (sessions) Lists sessions table converting destination IP
addresses to computer NETBIOS names.
-RR (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

RemoteName Remote host machine name.
IP address Dotted decimal representation of the IP address.
interval Redisplay selected statistics, pausing interval seconds
between each display. Press Ctrl+C to stop redisplaying
statistics.

C:\WINDOWS\system32>nbtstat -c

Ethernet (test):
Node IpAddress: [192.168.0.118] Scope Id: []

NetBIOS Remote Cache Name Table

Name Type Host Address
-----
OR<><><> <20> UNIQUE 192.168.0.118

C:\WINDOWS\system32>
```

```
Administrator: Command Prompt
C:\WINDOWS\system32>nbtstat -a 192.168.0.102

Ethernet (test):
Node IpAddress: [192.168.0.118] Scope Id: []

NetBIOS Remote Machine Name Table

Name Type Status
-----
RD-002 <00> UNIQUE Registered
EC<><><><> <00> GROUP Registered
RD-002 <20> UNIQUE Registered
MAC address :

C:\WINDOWS\system32>
```

Syntax of **nbtstat** command is:

```
C:\> Nbtstat [-a RemoteName] [-A IP address]
[-c] [-n] [-r] [-R] [-RR] [-s]
[-S] [interval]
```

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Sometimes when intruders gain remote access to a system, they try to find the other systems connected to the network and visible to the compromised system. To achieve this, the intruders create and execute batch files in the system and launch net view commands via SQL injection (by using a browser to send commands to the system through the web and database servers).

When the users establish connections with other systems using NetBIOS Networking, the systems maintain a list of other visible systems. By viewing the contents of the cached name table, the investigator might be able to determine other affected systems.

An Investigator should collect different kinds of network information to find evidences of the suspected incident. The network information useful for the investigation includes:

- Data content, like header information, text etc.
- Session information revealing particular data concerned to the investigation
- IDS/IPS log data
- Other network information like secure file transfers

Network data captured from various network areas includes information about:

- IDS/IPS or firewall logs
- Network protocols
- Server or application logs

- Tracing network packets
- Port scan results
- Live data capture

The NetBIOS name table cache maintains a list of connections made to other systems using NetBIOS Networking. It contains the remote system's name and IP address. You can use the Windows built-in command line utility Nbtstat to view the NetBIOS name table cache.

Nbtstat

Source: <http://technet.microsoft.com>


Nbtstat helps to troubleshoot NetBIOS name resolution problems. When a network is functioning normally, NetBIOS over TCP/IP (NetBT) resolves NetBIOS names to IP addresses. The syntax of the Nbtstat command is:

```
Nbtstat [ [-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S]
[interval] ]
```

Nbtstat with the **-c** switch shows the NetBIOS name table cache.

- **nbtstat -c**: This option shows the contents of the NetBIOS name cache, which contains NetBIOS name-to-IP address mappings.
- **nbtstat -n**: This displays the names that have been registered locally on the system by NetBIOS applications such as the server and redirector.
- **nbtstat -r**: This command displays the count of all NetBIOS names resolved by broadcast and by querying a WINS server.
- **nbtstat -S**: This option is used to list the current NetBIOS sessions and their statuses.

Network Connections

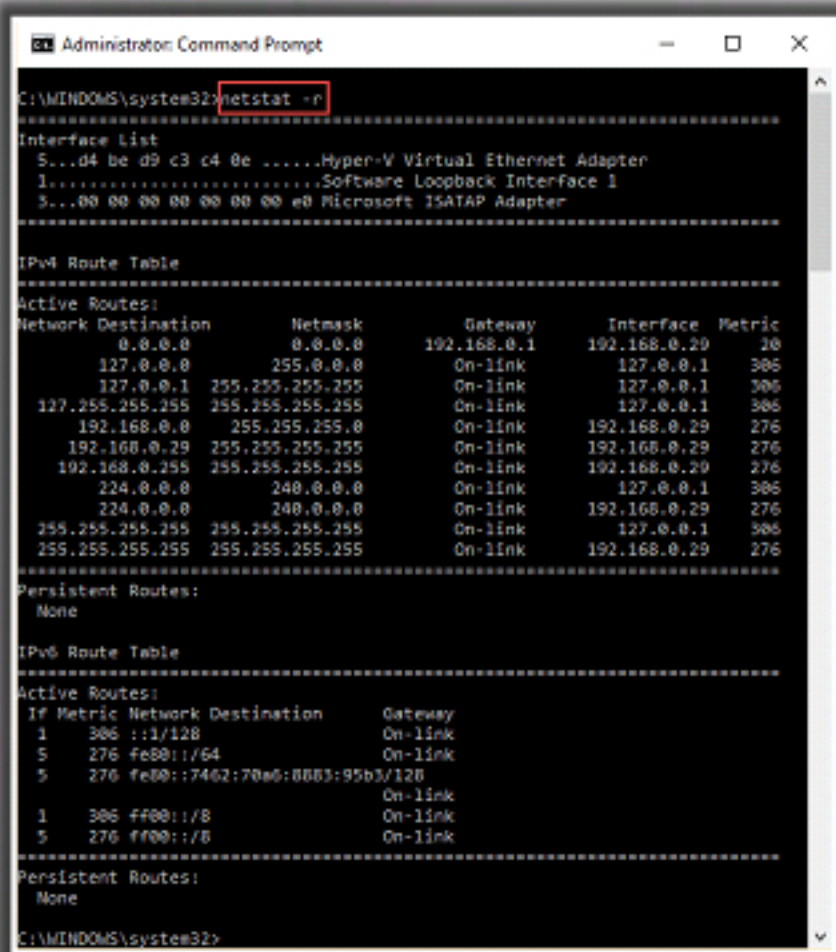


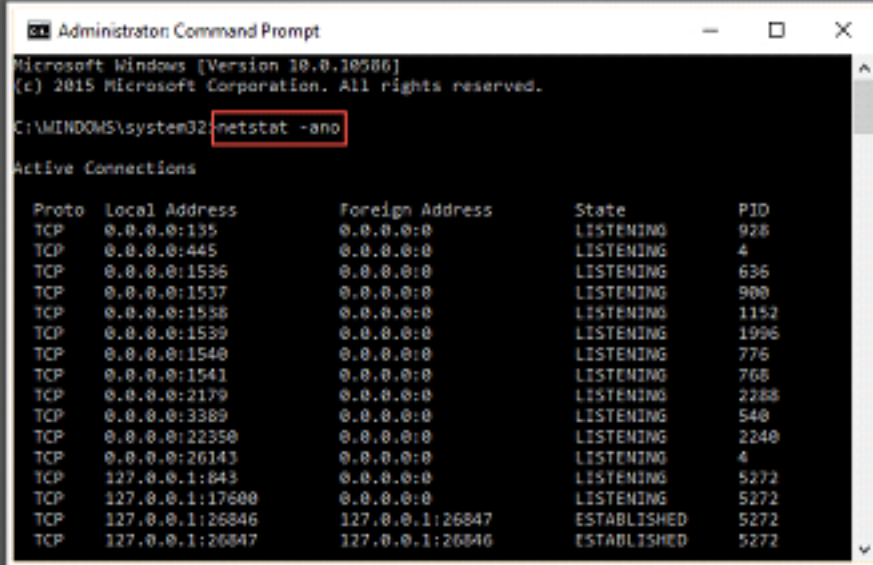
Collect information about the network connections running to and from the victim system, this allows to locate:

- Logged attacker
- IRCbot communication
- Worms logging into command and control server

Netstat with **-ano** switch displays details of the TCP and UDP network connections including listening ports, and the identifiers

Netstat with the **-r** switch displays details of the routing table and the frequent routes enabled on the system





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The investigator should collect information regarding network connections to and from the affected system, immediately after the report of any incident. If not done so, the information may expire over time.

The investigators should thoroughly observe the system and determine if the attacker has logged out, or is still accessing the system. It is also important to find out whether the attacker has installed any worm or IRCbot for communicating the data out of the system, and immediately search for other infected systems, updating itself, or logging into a command and control server. This information can provide important clues and add context to other information that the investigator has already collected.

Netstat

Source: <https://technet.microsoft.com>

Netstat tool helps in collecting information about network connections operative in a Windows system. This CLI tool provides a simple view of TCP and UDP connections, their state and network traffic statistics. Netstat.exe comes as a built-in tool with the Windows operating system. The most common way to run Netstat is with the **-ano** switches. These switches tell the program to display the TCP and UDP network connections, listening ports, and the identifiers of the processes (PIDs).

Using Netstat with the **-r** switch will display the routing table and show, if any persistent routes are enabled in the system. This could provide some useful information to an investigator or even simply to an administrator to troubleshoot a system.

Syntax


netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]

Parameters:

- **-a:** Displays all active TCP connections as well as the TCP and UDP ports on which the computer is listening.
- **-e:** Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.
- **-n:** Displays active TCP connections. However, the addresses and port numbers are expressed numerically with no specified names.
- **-o:** Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.
- **-p Protocol:** Shows connections for the protocol specified. In this case, the Protocol can be TCP, UDP, ICMP, IP, ICMPv6, IPv6 TCPv6, or UDPv6. Using this parameter with -s will display protocol based statistics. **-s:** Displays statistics by protocol. By default, this will show the statistics for the TCP, UDP, ICMP, and IP protocols. In case of installed IPv6 protocol, the tool displays statistics for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The use of -p parameter can specify a set of protocols.
- **-r:** Displays the contents of the IP routing table. This is equivalent to the route print command.
- **Interval:** Redisplays the selected information after the interval of defined number of seconds. Press CTRL+C to stop the redisplay. Omitting this parameter, will enable Netstat to print the selected information.

Using Netstat with the **-r** parameter will display the routing table and also show if the system has any persistent routes enabled. This provides some useful information for investigators and also administrators for troubleshooting the system.

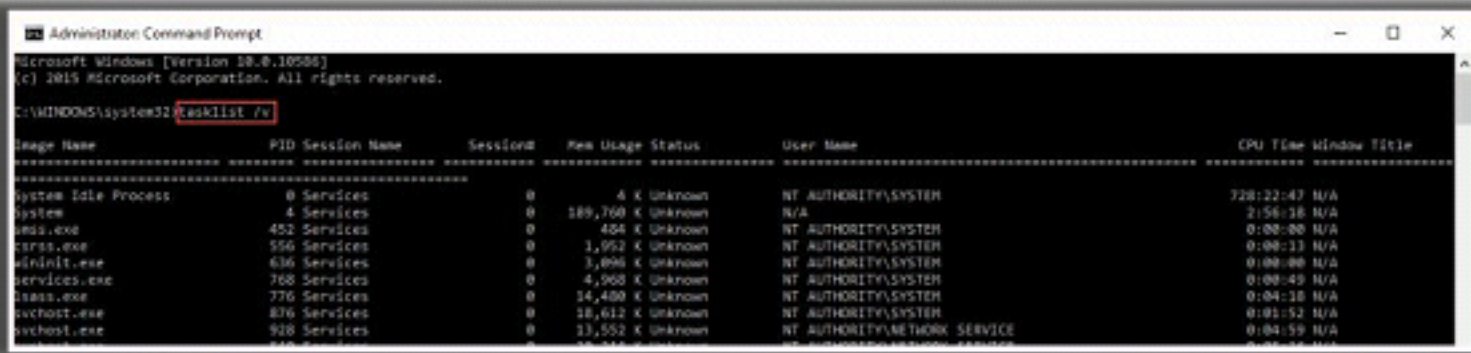
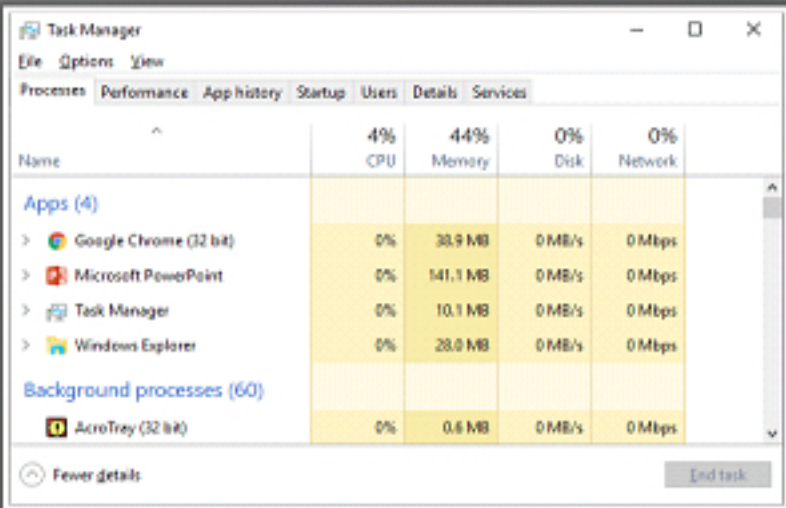
Process Information



- Investigate the **processes running on a potentially compromised system** and collect the information
- Tools and commands used to collect detailed process information include:

Task Manager displays the programs, processes, and services that are currently running on computer

Tasklist displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The investigators should gather information about all the processes running on the system. Use the Task Manager to view information about each process. However, the Task Manager does not display all the required information then and there. The investigator can retrieve the full process information by specifying few parameters listed below:

- The full path to the executable image (.exe file)
- The command line used to launch the process, if any
- The amount of time that the process has been running
- The security/user context that the process is running in
- The modules the process has loaded
- The memory contents of the process

Therefore, the investigators should learn to adopt certain other sources or tools and commands to collect the complete details of the process information. Tools and commands used to collect detailed process information include:

- **Tasklist**
- **Pstlist**
- **Listdlls**
- **Handle**

Tasklist

Source: <https://technet.microsoft.com>

Tasklist.exe, is a native utility included in Windows XP Pro and later versions, as a replacement for tlist.exe. The differences in the two tools are very fine, mostly being the name and the implementation of the switches. Tasklist.exe provides options for output formatting, with choices between table, CSV, and list formats. The investigator can use the /svc switch to list the service information for each process.

The Tasklist tool displays the list of applications and services along with the Process IDs (PID) for all tasks that running on either a local or a remotely connected computer.

Syntax: `tasklist[.exe] [/s computer] [/u domain\user [/p password]] [/fo {TABLE|LIST|CSV}] [/nh] [/fi FilterName [/fi FilterName2 [...]]] [/m [ModuleName] | /svc | /v]`

- **/s Computer:** Specifies the name or IP address of a remote computer (do not use backslashes).
- **/u Domain \ User:** Runs the command with the account permissions of the user specified by User or Domain\User.
- **/p Password:** Specifies the password of the user account that is specified in the /u parameter.
- **/fi FilterName:** Specifies the types of process (es) to include in or exclude from the query.
- **/m [ModuleName]:** Specifies to show module information for each process.
- **/svc:** Lists all the service information for each process without truncation.
- **/v:** Specifies that verbose task information be displayed in the output. Should not be used with the /svc or the /m parameter
- **/?:** Displays help at the command prompt

The /v (or verbose) switch provides the most information about the listed processes, including the image name (but not the full path), PID, name and number of the session for the process, the status of the process, the user name of the context in which the process runs, and the title of the window, if the process has a GUI.

Process Information (Cont'd)

Pslist

Pslist displays elementary information about all the **processes running** on a system.

Pslist-x

Pslist-x switch shows processes, memory information, and threads.

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32\C:\Users\Admin\Desktop\PSTools\pslist.exe

pslist v1.3 - Sysinternals PsList
Copyright (C) 2000-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for RD-006:
```

Name	Pid	Pri	Thd	Wnd	Priv	CPU Time	Elapsed Time
Idle	0	0	4	0	0	729:09:49.359	851:11:21.105
System	4	8	175	1415	644	2:56:23.625	851:11:21.105
smss	452	11	2	52	360	0:00:00.100	851:11:21.060
csrss	556	13	11	320	1392	0:00:13.734	851:10:37.077
wininit	636	13	1	138	1284	0:00:00.937	851:10:34.056
services	768	9	6	278	3268	0:00:49.500	851:10:26.653
lsass	776	9	8	1827	8464	0:04:18.196	851:10:26.626
svchost	876	8	26	891	10860	0:01:52.531	851:10:26.399
svchost	928	8	15	813	9316	0:04:59.406	851:10:26.322
svchost	540	8	41	1070	14756	0:05:17.187	851:10:26.062
svchost	800	8	31	813	14740	0:02:20.516	851:10:26.060

Administrator: Command Prompt

```
Name          Pid  VM  WS  Priv Priv Pk  Faults  NonP Page
Chrome        7676 258316 75408 43668 43964 45813 28 325
Tid Pri  Cswitch  State  User Time  Kernel Time  Elapsed Time
8016 4 28821  Wait:UserReq 0:00:01.109 0:00:00.375 2:57:47.022
8960 6 5055  Wait:Queue 0:00:00.078 0:00:00.062 2:57:45.928
8068 4 1  Wait:Queue 0:00:00.000 0:00:00.000 2:57:45.928
640 5 3291  Wait:UserReq 0:00:00.140 0:00:00.203 2:57:45.925
7292 5 9357  Wait:Unknown 0:00:00.156 0:00:00.031 2:57:45.924
8168 5 9050  Wait:Unknown 0:00:00.078 0:00:00.031 2:57:45.924
4852 4 5  Wait:Unknown 0:00:00.000 0:00:00.000 2:57:45.906
5380 4 31  Wait:UserReq 0:00:00.000 0:00:00.000 2:57:45.771
8460 4 15  Wait:UserReq 0:00:00.015 0:00:00.000 2:57:43.920
```

<https://technet.microsoft.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


Pslist.exe displays basic information about the already running processes on a system, including the amount of time each process has been running (in both kernel and user modes).

Parameters:

- -d: Shows thread detail
- -m: Shows memory detail
- -x: Shows processes, memory information and threads
- -t: Show process tree
- -s [n]: Runs in task-manager mode, for optional seconds specified
- -r n: Task-manager mode refresh rate in seconds (default is 1)
- \\computer: Shows information for the NT/Win2K system as specified
 - Add a username with parameter -u and password with -p to provide username and password of a remote system to log into it.
- -e: Exact match of the process name
- Pid: Instead of listing all the running processes in the system, this parameter narrows PsList scan for the specified PID

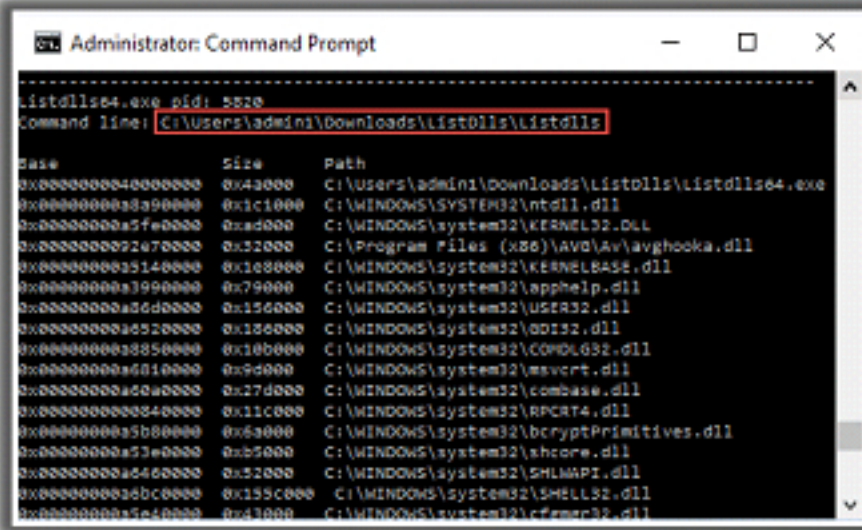
Source: <https://technet.microsoft.com>

Process Information (Cont'd)

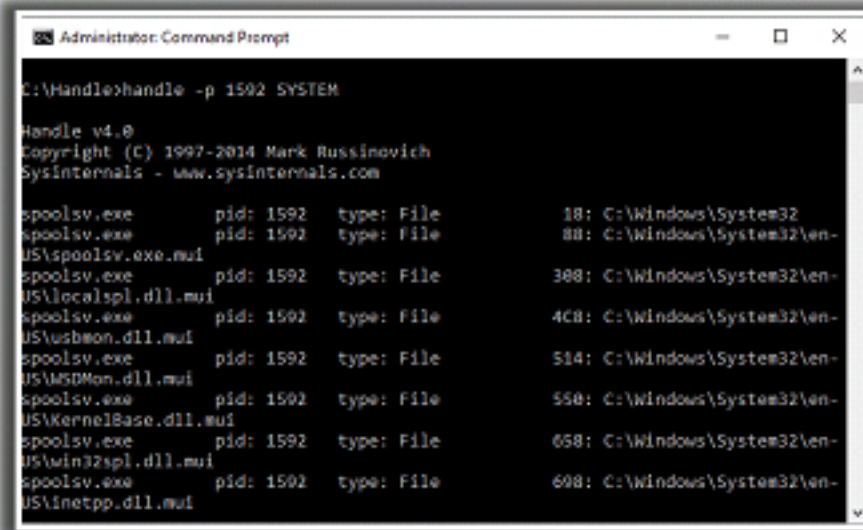


Listdlls

- Listdlls is a utility that lists all DLLs loaded in all processes, into a specific process, or to list the processes that have a particular DLL loaded
- It also displays **full version information for DLLs**, including their digital signature, and can be used to scan processes for unsigned DLLs



<https://technet.microsoft.com>



<https://technet.microsoft.com>

handle

- It displays information about open handles such as ports, registry keys, synchronization primitives, threads, and processes for any process
- This information is useful to determine the resources accessed by a process while it is running

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ListDLLs

ListDLLs is a utility that reports the DLLs loaded into processes. You can use it to list all DLLs loaded into all the processes, into a specific process, or to list the processes that have a particular DLL loaded. ListDLLs can also display full version information for DLLs, including their digital signature, and can also scan processes for unsigned DLLs.

Syntax:

```
listdlls [-r] [-v | -u] [processname|pid]
```

```
listdlls [-r] [-v] [-d dllname]
```

Parameters:

- **Processname:** Dump DLLs loaded by process (partial name accepted)
- **Pid:** Dump DLLs associated with the specified process id
- **Dllname:** Shows only processes that have loaded the specified DLL
- **-r:** Flags DLLs that relocated because they are not loaded at their base address
- **-u:** Lists unsigned DLLs
- **-v:** Shows DLL version information

The tool displays the full path of the loaded module as well as the version of the loaded DLL. By using this information, the investigators can find the actual code. Spyware, Trojans, and even

rootkits use a technique called DLL injection to load them into the memory space of a running process.

Handle

Handle is a utility that displays information about the open handles for any process in the system. You can use it to see the programs that have an open file or to see the object types and names of all the handles of a program. Other object types include ports, registry keys, synchronization primitives, threads, and processes. This information is useful to determine the resources accessed by a process while it is running

Handle helps in searching open file references, and find out whether the user has specified any command-line parameters; it will then list the values of all the handles in the system.

Syntax:

```
handle [[-a] [-u] | [-c <handle> [-l] [-y]] | [-s]] [-p <processname> | <pid>] [name]
```

-a	Dump information about all types of handles, not just those that refer to files.
-c	Closes the specified handle
-l	Dump the sizes of page file-backed sections.
-y	Don't prompt for close handle confirmation.
-s	Print count of each type of handle open.
-u	Show the owning user name when searching for handles.
-p	Instead of examining all the handles in the system, this parameter narrows Handle's scan to those processes that begin with the name process.
name	This parameter is present so that you can direct Handle to search for references to an object with a particular name.

TABLE 6.4: handle parameters

Source: <https://technet.microsoft.com>

Process-to-Port Mapping



- Process-to-Port Mapping **traces port used by the process**, and protocol connected to the IP
- Tools and commands to retrieve the process-to-port mapping:
 - 🌐 **Netstat command**

```
Administrator: Command Prompt
C:\WINDOWS\system32>netstat -o

Active Connections

Proto Local Address           Foreign Address         State       PID
TCP    127.0.0.1:26846          RD-006:26847           ESTABLISHED 5272
TCP    127.0.0.1:26847          RD-006:26846           ESTABLISHED 5272
TCP    192.168.0.29:28058      hk2sch130022039:https  ESTABLISHED 8040
TCP    192.168.0.29:28084      lon01:http             ESTABLISHED 1696
TCP    192.168.0.29:28280      maa03s18-in-f37:https  ESTABLISHED 9768
TCP    192.168.0.29:28288      162.125.17.3:https     ESTABLISHED 5272
TCP    192.168.0.29:28290      server-54-192-188-47:https CLOSE_WAIT 5272
TCP    192.168.0.29:28299      ec2-52-22-246-69:https CLOSE_WAIT 5272
TCP    192.168.0.29:28300      maa03s18-in-f14:https  ESTABLISHED 9768

C:\WINDOWS\system32>
```


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

When there is a network connection open on a system, then some processes must be using that connection, which means that every network connection and open port is associated with a process. Several tools are available, which the investigator can use to retrieve this process-to-port mapping. Use the following Netstat command to retrieve the process-to-port mapping.

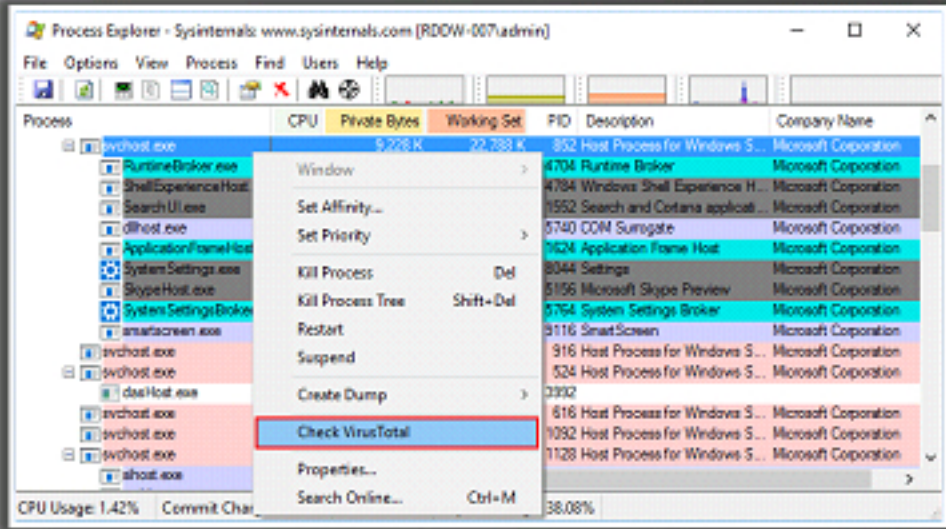
Netstat command

Netstat.exe offers the -o switch, which can display the process IDs for the processes responsible for the establishment of network connection. Once information is collected it needs to be correlated with the output of a tool such as tlist.exe or Tasklist.exe to determine the name of the processes using that particular network connection.

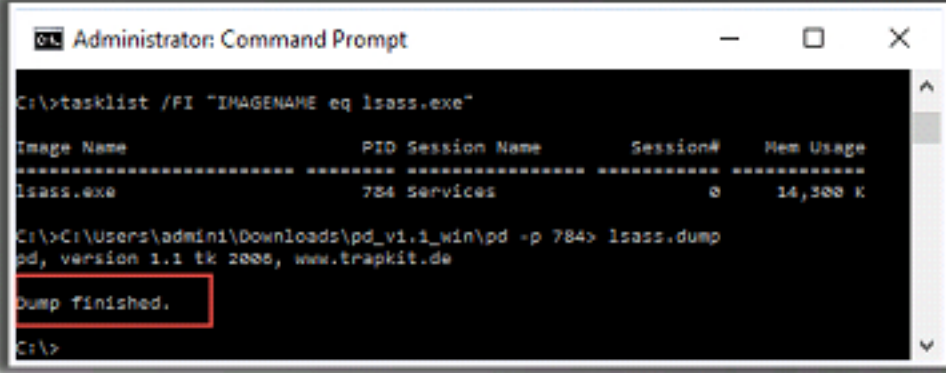
Process Memory



- Running processes could be **suspicious** or **malicious** in nature
- Process Explorer** program can be used to check if the process is malicious/suspicious
- Process Explorer shows the information about opened or loaded **handles** and **DLLs** processes
- If the process is suspicious, it gathers more information by dumping the memory used by the process using tools such as **PMDump**, **ProcDump**, **Process Dumper**, etc.
- The tool comes with built-in support for cross checking if the process is malicious by scanning it across the virustotal's malware database



<https://technet.microsoft.com>



<http://www.trapkit.de>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Process Explorer

Source: <http://technet.microsoft.com>

Process Explorer shows the information about the handles and DLLs of the processes, which have been opened or loaded. The Process Explorer display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in. If it is in handle mode, you will see the handles that are opened by the process selected in the top window; if the Process Explorer is in DLL mode, you will see the DLLs and memory-mapped files that the process has loaded.

PMDump

Source: <http://www.securityfocus.com>

PMDump is a tool that lets you dump the memory contents of a process to a file without stopping the process. This tool is highly useful in forensic investigations.

ProcDump

Source: <http://technet.microsoft.com>

ProcDump is a command-line utility. Its primary purpose is to monitor applications for CPU spikes and generating crash dumps during a spike so that an administrator or developer can determine the cause of the spike. ProcDump also includes hung window monitoring, unhandled


exception monitoring, and generating dumps based on the values of system performance counters.

Process Dumper (PD)

Source: <http://www.trapkit.de>

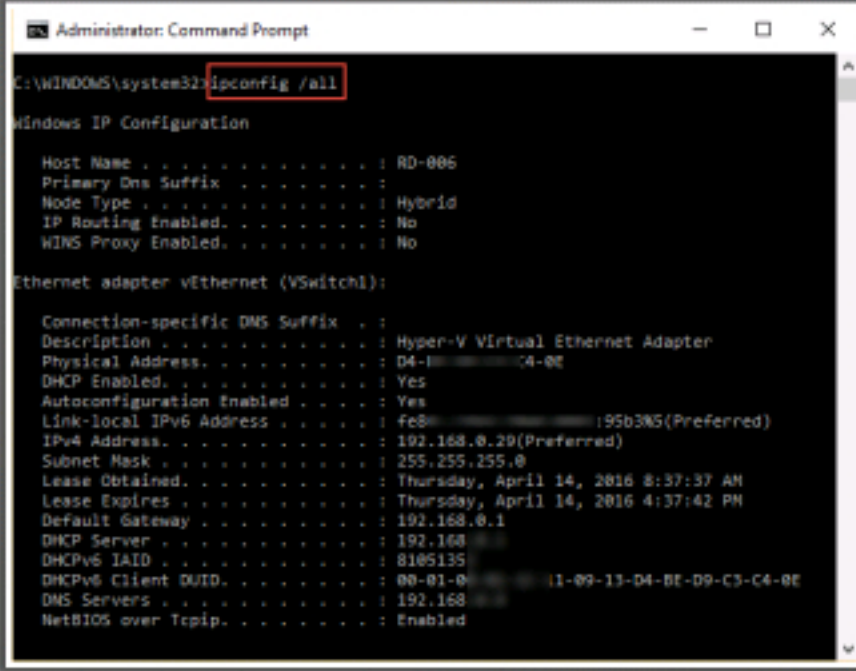
Process Dumper forensically dumps the memory of a running process. It is a command line interface tool that dumps the whole process space, uses meta-information to describe the different mappings, states, and saves the process environment.

Network Status



- Collect information of the **network interface cards** (NICs) of a system to know whether the system is connected to a **wireless access point** and what **IP address** is being used
- Tools for the network status detection are:
 - Ipconfig** command
 - PromiscDetect** tool
 - Promqry** tool

- Ipconfig.exe** is a utility native to Windows systems that displays information about NICs and their status
- Ipconfig /all** command displays the network configuration of the NICs on the system
- This information includes the state of the **NIC**, whether **DHCP** is enabled or not, the IP address of the NIC, etc.



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


The investigators should extract information about the status of the network interface cards (NICs) that connect a system with the available network. Currently, many laptops and desktops come with built-in wireless NICs, so that the information regarding the type of connection a device is using or the IP address it is using stays hidden. Gather the information about the status of NICs prior to acquiring the system in order to have better insight of the investigation results.

Ipconfig command

Ipconfig.exe is a command line utility, which the investigator can use to find out information about NICs and the current Transmission Control Protocol/Internet Protocol (TCP/IP) configuration. Ipconfig also accepts various Dynamic Host Configuration Protocol (DHCP) commands, thereby allowing a system to update or release its TCP/IP network configuration.


Investigators should use the **ipconfig /all** command to view all the current TCP/IP configuration values including the IP address, subnet mask, default gateway and Windows Internet Naming Service (WINS) and DNS configuration. The information generated by this command also includes the state of the NIC and DHCP. This information will help the investigators to examine the network traffic logs and the IP address of the systems involved.

Network Status (Cont'd)



PromiscDetect checks if network adapter(s) is running in promiscuous mode, which may be a sign that a sniffer is running on computer

Promqry is a command line tool used to detect network interfaces that are running in promiscuous mode



```
Administrator: Command Prompt
C:\>C:\Users\admin1\Downloads\PromiscDetect\promiscdetect.exe

PromiscDetect 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- http://ntsecurity.nu/toolbox/promiscdetect/

Adapter name:
- Realtek PCIe GBE Family 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)
- All multicast (capture all multicast packets)
- Broadcast (capture broadcast packets)
- Promiscuous (capture all packets on the network)

http://ntsecurity.nu
```

```
Administrator: Command Prompt
C:\>C:\Users\admin1\Downloads\promqry

Querying local system...

Active: True
InstanceName:
Hyper-V Virtual Ethernet Adapter
NEGATIVE: Promiscuous mode currently NOT enabled

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

Active: True
InstanceName:

http://www.microsoft.com
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers install sniffer on the compromised systems in order to capture network traffic information such as login credentials, or to map the services other systems connected to the network are running. NICs can capture network traffic data only when they are in promiscuous mode.

An administrator or investigator will not be able to directly find out whether the NIC is in promiscuous mode or not, because the systems have no special button or icon to indicate the NIC mode. Furthermore, the systems do not have any tray icon or Control Panel setting that can directly indicate if someone is sniffing the network traffic.

Therefore, investigators need to use special tools to detect such incidents and programs that may be running on a system. Tools such as PromiscDetect and Promqry can help in analyzing the NIC status of the system.

PromiscDetect

Source: <http://ntsecurity.nu>

PromiscDetect checks if the network adapter(s) is running in promiscuous mode, which may be a sign that there is a sniffer running on the computer.

Promqry

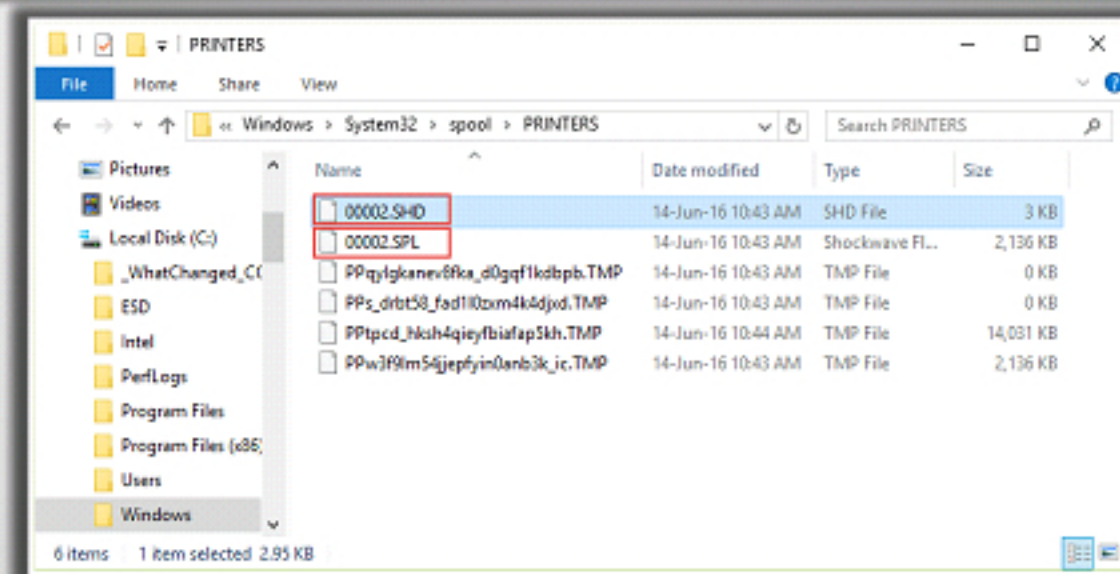
Source: <https://www.microsoft.com>

Promqry can determine if a Windows system has network interfaces in promiscuous mode. If a system has network interfaces in promiscuous mode, it may indicate the presence of a network sniffer running on the system. It has command line and GUI versions. Users can run the tool using any of the versions and dump its output to a text file. It cannot detect standalone sniffers or sniffers running on non-Windows operating systems.

Print Spool Files



- Print spooler is a **software program** for managing current print jobs
- Creates a temporary **folder** containing the print tasks with '**SPL**' and '**.SHD**' extension files
- The system deletes these files after completing the task
- The temporary files can store print details such as owner, document, printer, printing processor - format, number of copies printed and the print method
- The windows printing process supports **two data types**:
 - RAW** - .SPL file consists of data to be printed
 - EMF** - .SPL file consists the metadata and can be printed on any printer
- By default, the path of .SPL and .SHD in windows is **C:\Windows\System32\spool\PRINTERS**



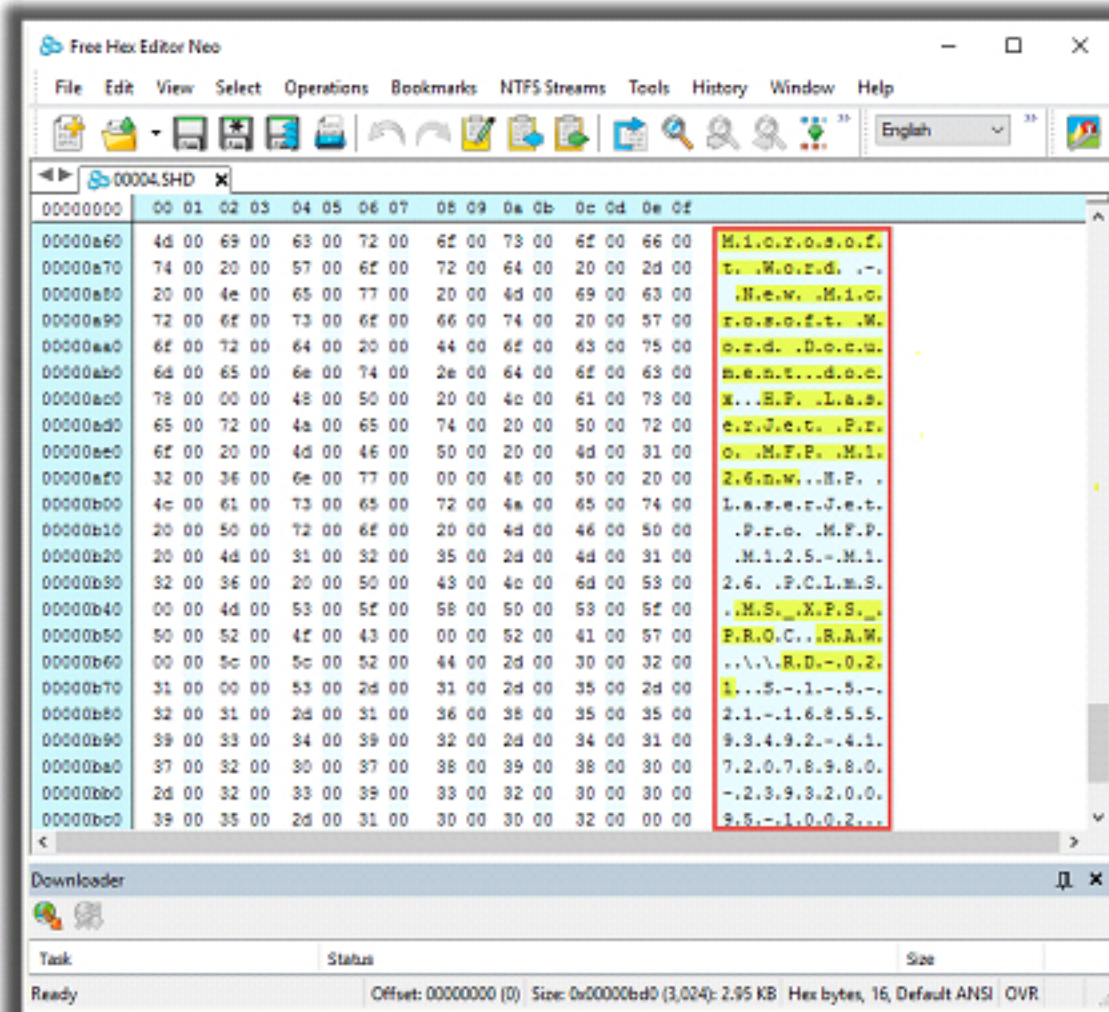
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Print Spool Files (Cont'd)



- SPL and .SHD files contain **metadata** stored as **Unicode** and require Unicode capable tools to explore:

- Hex editors
- UCHECK



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Print spool refers to a software program, which manages all print jobs in a Windows system. It stores the data that the user wants to print in a temporary manner, until the printer completes its jobs. It helps the users to manage the print job during processing or otherwise manage incomplete print jobs.

Print spool files are the temporary files that the software program stores in the system, before completing the print task or to start printing at a scheduled time. Windows stores the file in print spooler directory before printing, while the local print provider (Localspl.dll) writes the contents to a spool file (.spl) and creates a separate graphics file (.emf) for each page. Localspl.dll also maintains the detailed data on a print job in a shadow file (.shd) like the username, filename, etc.

By default, in Windows operating system the .SPL and .SHD files are stored in the spool folder driver in C:\Windows\System32\spool\PRINTERS folder. Based on the printer configuration, the print jobs can also be spooled in Windows virtual memory. The system deletes the .spl, .shd and .emf files after completion of the task.

These files help the investigators to find useful information in case the system or network had a printer connected during the incident, and also if it was disconnected after the incident. The xxx.shd represents a shadow file and xxx.spl represent spool file, and xxx represents print job number. The .shd file contains details of the printed file such as name of the printed file, location, name of the printer used and timestamp.

Other Important Information



Clipboard Contents

- It is the memory area which stores the data for future use
- This data found in the clipboard can be used in a variety of cases such as information or intellectual property theft, fraud, or harassment.



Service/Driver Information

- When the system starts, services and drivers start automatically based on entries in the registry
- Users/system admins do not install all the services, some malware installs itself as a service or system driver
- Check service/driver information for any malicious program installed



Path	Name	ProcessId	StartMode	State	Status
\\.\system32	AdobeFlashPlayerUpdateSvc	2072	Auto	Running	OK
\\.\system32	AdobeFlashPlayerUpdateSvc	0	Manual	Stopped	OK
\\.\system32	AlRouter	0	Manual	Stopped	OK
\\.\system32	AlRouter	0	Manual	Stopped	OK
\\.\system32	AppIDSvc	0	Manual	Stopped	OK
\\.\system32	AppInfo	1128	Manual	Running	OK
\\.\system32	AppMgmt	0	Manual	Stopped	OK
\\.\system32	AppReadiness	0	Manual	Stopped	OK
\\.\system32	AppVClient	0	Disabled	Stopped	OK
\\.\system32	AppXSvc	0	Manual	Stopped	OK
\\.\system32	AudioEndpointBuilder	524	Auto	Running	OK
\\.\system32	AudioSrv	1428	Auto	Running	OK
\\.\system32	Browser	1128	Manual	Running	OK
\\.\system32	Browser	0	Manual	Stopped	OK
\\.\system32	CDPSvc	1136	Auto	Running	OK
\\.\system32	CertPropSvc	0	Manual	Stopped	OK
\\.\system32	Clipboard	5620	Manual	Running	OK
\\.\system32	COMSysApp	0	Manual	Stopped	OK
\\.\system32	ComMessagingRegistrar	1002	Auto	Running	OK

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Clipboard Contents

Clipboard is a temporary storage area, where the system stores data during copy and paste operations. Most Windows applications provide this functionality through the Edit option on the menu bar. Clicking Edit reveals a drop-down menu, which contains choices, like cut, copy, and paste. The user selects text or other data, chooses copy, and then chooses Paste to insert that data somewhere else. The cut functionality removes the data from the document the user is working on, and that data goes to the clipboard.

When a user performs any cut/copy function, and then pastes the content into the document, the information cut/copied is copied to the clipboard and as long as the computer has uninterrupted power supply or the user does not log out, the system neither adds nor deletes the clipboard contents.

Attackers use edit options to copy information from the system to various other sources, such as removable media, documents, email, etc. Investigators can retrieve the copied data from the clipboard contents, by using various clipboard extraction tools.

Free Clipboard Viewer

Source: <http://www.freeclipboardviewer.com>

Free Clipboard Viewer is a program used to view the information that is stored in memory when you use copy and cut functions in Windows operating system. A clipboard viewer displays the current content of the clipboard.


Free Clipboard Viewer allows you to save the clipboard data to a file and also load clipboard data from a file, so that you can transfer clipboard contents between computers.

Service/Driver Information

Based on the entries in the registry the services and drivers start automatically when the system is started. Most users do not even see these running services as processes, because there are really no obvious indications, as there are with regular processes. Yet, these services run nonetheless. The user or even the system administrators necessarily do not install all the services. Some malwares installs themselves as a service or even as a system driver. Check service/device information for any malicious program installed.

Investigators can gather services information using the tasklist command line tool. The tool will display image name and related PID services. The investigators can also use the Windows Management Instrumentation Command (wmic) in the following way to view the list of running services, their process IDs, startmode, state and status.

Other Important Information (Cont'd)

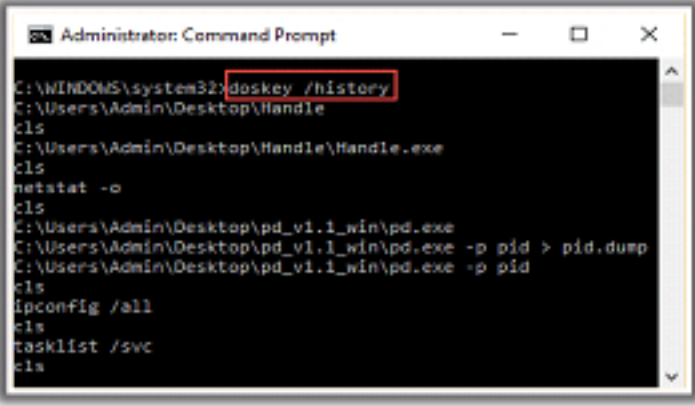


Command History

- Use the **doskey /history** command to see previously typed commands

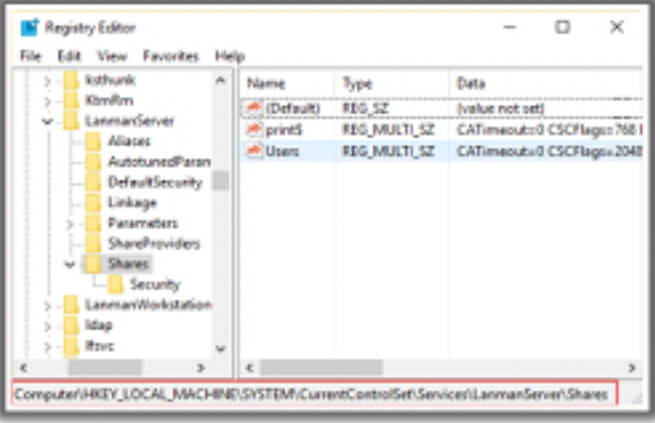
Mapped Drives

- Drives could be **mapped** with a malicious intent
- Drive mappings can be **correlated to network connection** information retrieval



Shares

- Gets the information regarding the shared resources
- This information is maintained in a folder:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Command History

At the time of investigation, if there are too many command prompts, the commands typed by the user, such as ftp or ping, could hide valuable clues. To see the previously typed commands, the investigator can run the scroll bar for the command prompt up. If the user typed the **cls** command to clear the screen, the investigator would not be able to use the scroll bar to see any of the commands that the user had entered. Instead, the investigator should use the **doskey /history** command, which shows the history of the commands typed into that prompt.

Mapped Drives

During the investigation, the investigator might want to know what drives or shares the target system has mapped to. The user could have created these mappings, and they might provide information regarding the indication of malicious intent. There might be no persistent information within the file system or registry for these connections to the mapped shares on other systems.

Shares


Besides resources used by the system, an investigator also wants to acquire information regarding the resources that the system is making available to other users over the network. The system stores the information about shared files and folders in the following registry root key:


HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Shares




Non-volatile data is a sort of permanent data that would remain on the system even after the use switches it off, but the system is easy to manipulate through online and direct access. Therefore, investigators must either extract or copy the non-volatile data from the system.

Collecting Non-Volatile Information







Non-volatile data remain **unchanged** when a system is shut down or be unable to find power



Example: Emails, word processing documents, spreadsheets and various “deleted” files



Such data usually resides in **hard drive** (swap file, slack space, unallocated drive space, etc.)



Other non-volatile data sources include DVDs, **USB thumb** drives, smartphone’s memory, etc.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Volatile information gathering is not the only aim of the investigator. Investigators need detailed information; because evidence is the only thing that helps them to solve the case with ease. They need to have firm evidences based on both volatile and nonvolatile data.

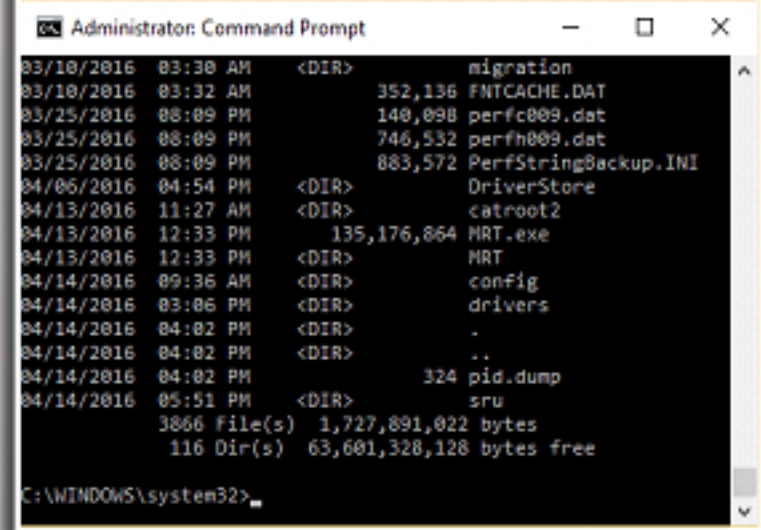
Nonvolatile data remains unchanged when a system shuts down or loses power. Some of the examples of nonvolatile data include emails, word processing documents, spreadsheets, and various “deleted” files. The investigator can decide what information needs to be extracted from the registry or what information about (or from) files should be collected for additional analysis.

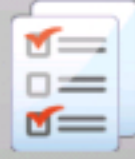

There is also a possibility that the attacker could be actively logged into the system and accessing the data. In such cases, the investigator may decide to even track the attacker. It is important that the investigator should preserve certain important information intact without any modification or deletion. Once the user starts the system, there may be some data modifications, such as drives mapped to or from the system, services started, or applications installed. These modifications might not be persistent across a reboot and therefore, the investigator should record and document them. Non-volatile data usually resides in the hard drives; it also exists in swap files, slack space, and unallocated drive space. Other non-volatile data sources include CD-ROMs, USB thumb drives, smart phones, and PDAs.

Examine File Systems

- Run the command **dir /o:d** in command prompt
- Enables the investigator to examine:
 - The **time** and **date** of the OS installation
 - The service packs, patches, and sub-directories that automatically update themselves often. For e.g.: drivers, etc.
- Give priority to recently dated files





Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Understanding file systems is imperative to access to the file system data and to rebuild the file system events. File systems comprise of five sections, namely, file system data, content data, metadata, file name, and file system application data.

File system data

The file system data gives details about the file system structure, like file system and file system block size, number of allocated blocks etc.

Content data

This data has most of the information of the file system. It consists of the content of the file system.

Meta data


The Meta data of the file system generally provides information about content locations, file size and MAC timestamps.

Application data

The application data gives information about the File system journal Quota statistics.

All the above information of the file systems enables the investigator to collect a variety of data, which may contain potential evidences for solving the case.

Registry Settings



- Several registry values and settings could effect the subsequent forensic analysis and investigation
- **Registry Editor** utility can be used to access and manage the Registry
- Registry values that can greatly affect an investigation are following:

ClearPageFileAtShutdown	DisableLastAccess	AutoRuns
<ul style="list-style-type: none"> 🟢 This registry value tells the operating system to clear the page file when the system is shut down 🟢 The information within the page file remains on the hard drive during the system shut down. This can be portions of IM conversations, decrypted passwords, and other strings and bits that might provide important clues in the investigation 🟢 Clearance of page file during the shutdown cause difficulty to obtain that valuable information 	<ul style="list-style-type: none"> 🟡 In Windows 10, you can set the value of <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate</code> key to 1 to disable updating of the last access times on files 🟡 On Windows 10, you can also run fsutil command in an elevated command prompt to query, enable, or disable "Last Access Time" 	<ul style="list-style-type: none"> 🔒 Several areas of the Registry are referred as autostart locations since they provide the ability to automatically start applications. 🔒 Locations can start the applications automatically at the time of system boots, user logs in, and when-the user takes a specific action. 🔒 Collect the information from specific keys and values with the help of reg.exe tool or AutoRuns tool, as part of the first-response activities.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Registry values and settings have significant impacts on the subsequent forensic analysis and investigation. Although these settings are non-volatile themselves, but they affect how an investigator chooses to proceed while conducting an investigation or even whether he or she would continue with the investigation at all. There are several tools for collecting information from the registry. Reg.exe is a command line tool for accessing and managing the registry. Some of the important registry values to note down include:

ClearPageFileAtShutdown

This particular registry value tells the operating system to clear the page file when the system is shut down. Since Windows uses virtual memory architecture, some memory used by processes will be paged out to the page file. When the system shuts down, the information within the page file remains on the hard drive and contains information such as decrypted passwords, portions of IM conversations, and other strings and bits of information that might provide important leads in an investigation. However, if the system clears the file during shutdown, there is a chance that the information may be deleted and then this valuable information will be more difficult to obtain.

DisableLastAccess

Windows has the ability to disable the updating of the last access times on files. This feature is actually meant for performance enhancement, particularly on high-volume file servers. In case of normal workstations with desktops and laptops, this setting does not provide any noticeable improvement in performance.

Users can query or enable this setting via the **fsutil** command. For example, to query the setting, use this command:

```
C:\>fsutil behavior query disablelastaccess
```

Fsutil

Source: <https://technet.microsoft.com>

This command performs the tasks that are related to file allocation table (FAT) and NTFS file systems, such as managing reparse points, managing sparse files, or dismounting a volume. If it is used without parameters, fsutil displays a list of supported subcommands. The investigator must be logged on as an administrator or a member of the administrators group in order to use fsutil.

AutoRuns Tool

There are several areas of the registry (and the file system) referred to as autostart locations, because they provide a facility to automatically start applications, usually without any direct interaction from the user. Some of these locations will automatically start applications when the system boots, while others do so when a user logs in, and still others when the user takes a specific action. In such instances users start an application, and they are completely unaware that they have actually launched another hidden application.

Investigators can collect this information by two means: one by using the reg.exe tool, and the other with the AutoRuns tool.

AutoRuns is also a great tool for checking areas within the file system, such as scheduled tasks. Occasionally, administrators use scheduled tasks feature to provide themselves with elevated (i.e., system level) privileges, to perform tasks like viewing portions of the registry that are normally off limits even to administrators. An attacker who gains administrator-level access into the system may try to do something similar to this feature so that he can extend his presence on the system.

Another area of the registry that can provide valuable information in an investigation is the protected storage area. The protected storage holds information in an encrypted format in the registry. If an investigator acquires an image of the system, tools such as AccessData's Forensic ToolKit (FTK) will decrypt and recover the information.

Microsoft Security ID



- Microsoft Security IDs are available in **Windows Registry Editor**
- The path to access IDs is:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList**



Name	Type	Data
(Default)	REG_SZ	(value not set)
Default	REG_EXPAND...	%SystemDrive%\Users\Default
ProfilesDirectory	REG_EXPAND...	%SystemDrive%\Users
ProgramData	REG_EXPAND...	%SystemDrive%\ProgramData
Public	REG_EXPAND...	%SystemDrive%\Users\Public

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Microsoft Security ID refers to a unique identification number that Microsoft assigns to a Windows user account for granting the user access to a particular resource. In Windows, when a user logs on, the system gathers SID from the database and uses it as access token to identify the user in all the aspects of Windows security. This token consists of privileges granted to the user, based on which the system will allow or deny access.

Event Logs



- Event logs can change rapidly depending on the **configuration and audited events**
- Choose which data have to be collected depending on the **occurred instance**
- Use tools such as **psloglist.exe** to retrieve the event records
- Copy the event log files (**.evt files**) themselves off the system

```
Administrator: Command Prompt

[011] Microsoft-Windows-Ntfs
Type: INFORMATION
Computer: RD-006
Time: 1/4/2016 11:35:09 AM ID: 98
User: NT AUTHORITY\SYSTEM
Message text not available. Insertion strings:
C:\Device\HarddiskVolume2 0

[010] Microsoft-Windows-Ntfs
Type: INFORMATION
Computer: RD-006
Time: 1/4/2016 11:35:09 AM ID: 98
User: NT AUTHORITY\SYSTEM
Message text not available. Insertion strings:
\\?\Volume{55706ef9-801d-11e1-a709-806e6f6e6963} \Device\HarddiskVolume1 0

[009] Microsoft-Windows-FilterManager
Type: INFORMATION
Computer: RD-006
Time: 1/4/2016 11:35:09 AM ID: 6
User: NT AUTHORITY\SYSTEM
File System Filter 'Wof' (10.0, 2015-10-30T08:08:16.000000000Z) has successfully loaded and registered with Filter Manager.

[008] Microsoft-Windows-FilterManager
Type: INFORMATION
Computer: RD-006
Time: 1/4/2016 11:35:09 AM ID: 6
User: NT AUTHORITY\SYSTEM
File System Filter 'FileInfo' (10.0, 2015-10-30T08:07:17.000000000Z) has successfully loaded and registered with Filter Manager.
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


Event logs are essential files within the file system. These files are changeable in nature. In fact, depending on how their configuration and events are audited, these files can change quite rapidly. Depending on the audit policies on the “victim” system and the investigators accessing it as the first responder, the system generates entries stored within the event logs. Use tools such as psloglist.exe to retrieve the event records.

PsLogList

Source: <http://technet.microsoft.com>

PsLogList allows to login to remote systems in situations when current set of security credentials would not permit access to the Event Log. It retrieves message strings from the computer on which the event log resides. It shows the contents of the System Event Log on the local computer and allows formatting of Event Log records.

ESE Database File



- Windows 10 comes with **Microsoft Edge** as default web browser
- It uses the **Extensible Storage Engine (ESE) database** format to store browsing records, including history, cache, and cookies
- The database store tables - FileCleanup, Folder, ReadingList, RowId, MSysObjids, MSysObjects, FolderStash, MSysLocales, and MSysObjectsShadow

Common artifact locations of Microsoft Edge include:

- ESE database:
`\Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_XXXX\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\XXXX\DBStore\spartan.edb`
- Edge cached files location:
`\Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_XXXX\AC\#1001\MicrosoftEdge\Cache\`
- Edge last active browsing session data location:
`\Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_XXXX\AC\MicrosoftEdge\User\Default\Recovery\Active\`
- Edge stores history records, Cookies, HTTP POST request header packets and downloads in:
`\Users\user_name\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat`
- If the last browsing session open was in Private mode then the browser stores these records in:
`\Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_XXXX\AC\MicrosoftEdge\User\Default\Recovery\Active\{browsing-session-ID}.dat`

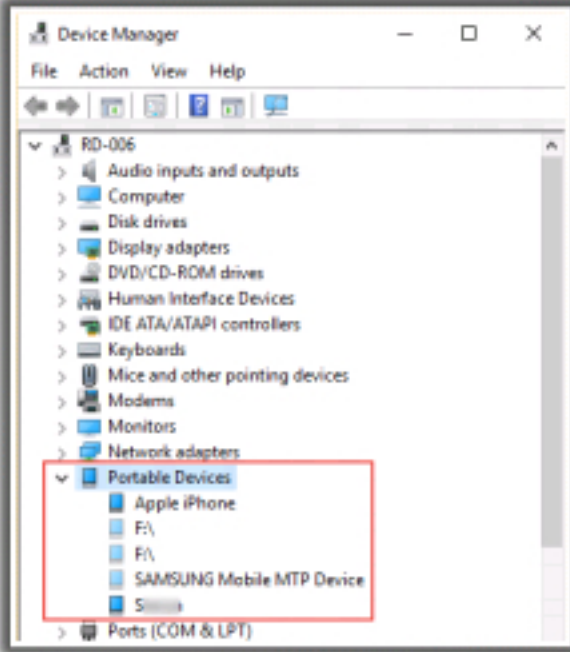
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows 10 has the Microsoft Edge browser as a built-in feature. It uses the Extensible Storage Engine (ESE), which is a data storage technology from Microsoft, made to store and retrieve data sequential access. This database storage helps the server to store various files, messages etc. and access folders, text messages, attachments, etc. for email service provision. These files have the extension .edb and can provide valuable case evidences in forensic investigations. The database is in the form of a B-Tree structure and has a hexadecimal file signature.

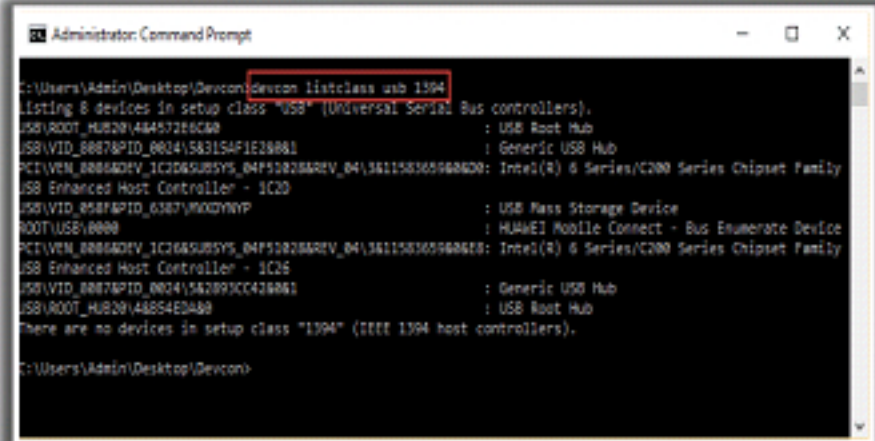
The database stores tables, categorized as FileCleanup, Folder, ReadingList, RowId, MSysObjids, MSysObjects, FolderStash, MSysLocales, and MSysObjectsShadow. These tables contain information of all the applications stored and accessed from the system. This information can act as evidence in case of criminal incidents.

Connected Devices

- Document devices connected to a system undergoing investigation
- Recently connected devices can be find manually
- Go to **Control Panel** and click **Hardware and Sound**
- In the **Devices and Printers** section, click **Device Manager**
- In the Device Manager window, click on **View** in the toolbar and select "**Show hidden devices**"
- To view the connected portable devices double-click the **Portable Devices**



- **DevCon** tools can be used to document devices that are attached to a Windows system
- The output of **DevCon resources=ports** and **DevCon listclass USB 1394**



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

DevCon


DevCon or Device Console, is a command-line tool that displays detailed information about devices on computers running Windows operating system. DevCon can be used to enable, disable, install, configure, and remove devices. It also performs device management functions on local computers and remote computers.

Features:

- Display driver and device info
- Search for devices
- Change device settings
- Restart the device or computer

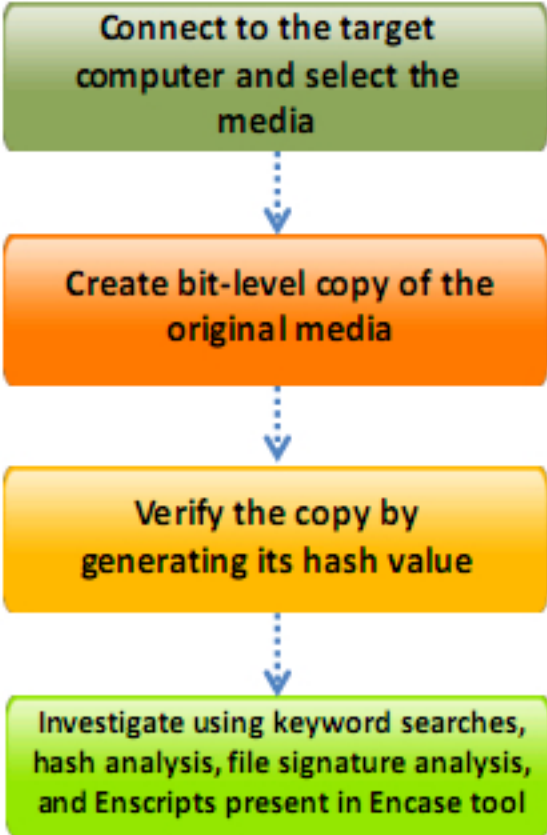
Source: <https://msdn.microsoft.com>

Slack Space



- Slack space refers to the **portions of a hard drive** which may contain data either from a previously deleted file or unused by the currently allocated file
- Non-contiguous** file allocation leaves more trailing clusters leaving more slack space
- The data residue in the slack space is retrieved by **reading the complete cluster**
- DriveSpy** tool collects all the slack space in an entire partition into a file

Steps in slack space information collection




```
graph TD; A[Connect to the target computer and select the media] --> B[Create bit-level copy of the original media]; B --> C[Verify the copy by generating its hash value]; C --> D[Investigate using keyword searches, hash analysis, file signature analysis, and Encscripts present in Encase tool];
```

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

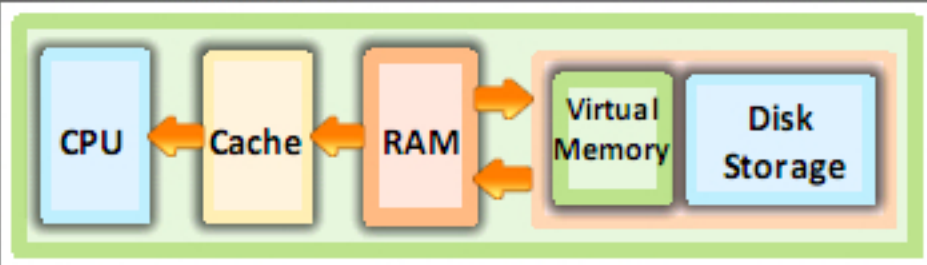
Slack space, also called file slack, is the space generated between the end of the file stored and the end of the disk cluster. This happens when the size of the file currently written is less than that of the previous written file on the same cluster. In such cases, the residual data remains as it is, and may contain meaningful information when examined forensically.

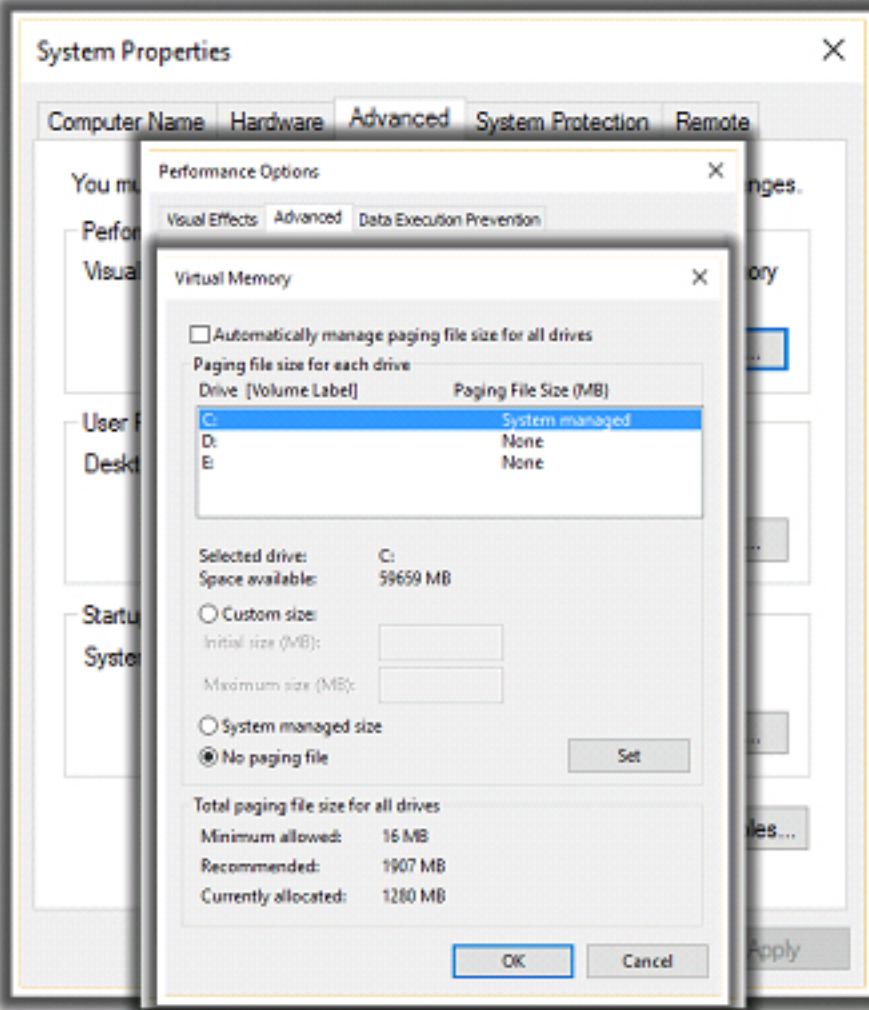
It may be possible to use slack space to store data that one wants to hide without having knowledge of the underlying file system. In order to do that you just have to make a file smaller than the slack space present and use the rest of space to store the hidden data. This data will be invisible to the file system and remains the same until changed manually. However, creating new files that result in slack space is not the safest way to hide data.

Virtual Memory



- Virtual (or logical) memory is a concept that, when implemented by a computer and its OS, allows programmers to use a **large range of memory addresses** for stored data.
- Virtual memory can be scanned to find out the **hidden running processes**.
- Use **X-Ways Forensics** tool to scan virtual memory.





Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

X-Ways Forensics is a computer forensics tool that has the following features:

- Access logical memory of running processes
- Gather slack space, free space, inter-partition space, and generic text from drives and images
- Ability to read partitioning and file system structures
- Memory analysis for local RAM or memory dumps
- Disk cloning and imaging

Source: <http://www.x-ways.net>

Hibernate Files



- Hibernate file is the snapshot of the **RAM data**, created when the system **hibernates**
- Stored in HDD as **hiberfil.sys**
- Helps investigator to:
 - ⦿ Track the list of **applications**
 - ⦿ Compare **RAM's live image**
 - ⦿ Find the local and remote **authentication** details
 - ⦿ Create a **keyword list** for brute force attempts to login sessions
 - ⦿ To find more information on the investigation of **Hibernation slack space**
- Tools used to explore **hiberfil.sys**:
 - ⦿ Hex Editor
 - ⦿ AccessData's FTK
 - ⦿ MoonSols Windows Memory Toolkit

Byte Offset	Structure	Attributes
0x0	Signature	[String, {length: 4}] (PostVista) "WAKE" "HIBR" "RSTR" (PreVista) "wake" "hbr" "rstr"
0x4	Version	[unsigned long]
0x8	Checksum	[unsigned long] Set to 0 = MS Boot Loader does not check compressed pages
0xc	LengthSelf	[unsigned long]
0x10	PageSelf	[unsigned long]
0x14	PageSize	[unsigned long]
0x18	SystemType (ImageType)	[unsigned long]
0x20	SystemTime	[winTimeStamp, {}]
0x28	InterruptTime	[unsigned long long]
0x30	FeatureFlags	[unsigned long]
0x34	HiberFlags	[unsigned char]
0x35	Spare	[array, 3, [unsigned char]]
0x38	NextHiberPtes	[unsigned long]
0x3e	HiberVa	[unsigned long]
0x40	HiberPte	[LARGE_INTEGER]
0x48	NextFreePages	[unsigned long]
0x4c	FreeMapCheck	[unsigned long]
0x50	WakeCheck	[unsigned long]
0x54	TotalPages	[unsigned long]
0x58	FirstTablePage	[unsigned long] Pointer to the first memory table
0x5c	LastFilePage	[unsigned long]
0x60	PerfInfo	[PO_HIBER_PERF] Introduced in Windows XP
	NextBootLoaderLogPages	Introduced in Windows Vista
	BootLoaderLogPages [8]	Introduced in Windows Vista
	TotalPhysicalMemoryCount	

Section	Subsection	Type
PointerSystemTable	-	DWORD
NextTablePage	-	UINT32
Checksum	-	DWORD
EntryCount = 255	-	UINT32
MemoryTableEntries[EntryCount]	PageCompressedData	UINT32
	PhysicalStartPage (Location of the memory range)	UINT32
	PhysicalEndPage (Location of the memory range)	UINT32
	Checksum	DWORD

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows operating system has two power management modes. First is the Sleep Mode, which keeps the system running in a low power state so that the user can instantaneously get back where he/she has paused working. The second power management mode is the Hibernate mode, which completely writes the memory as a hiberfil.sys file in HDD.

In the forensic point of view the hiberfil.sys file is a crucial source of evidence, as it consists of the crucial information of all programs, applications, files and processes that were running on the RAM at a given time.

Investigators can check if the user had enabled hibernate option by visiting the following registry key in the registry editor:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power.

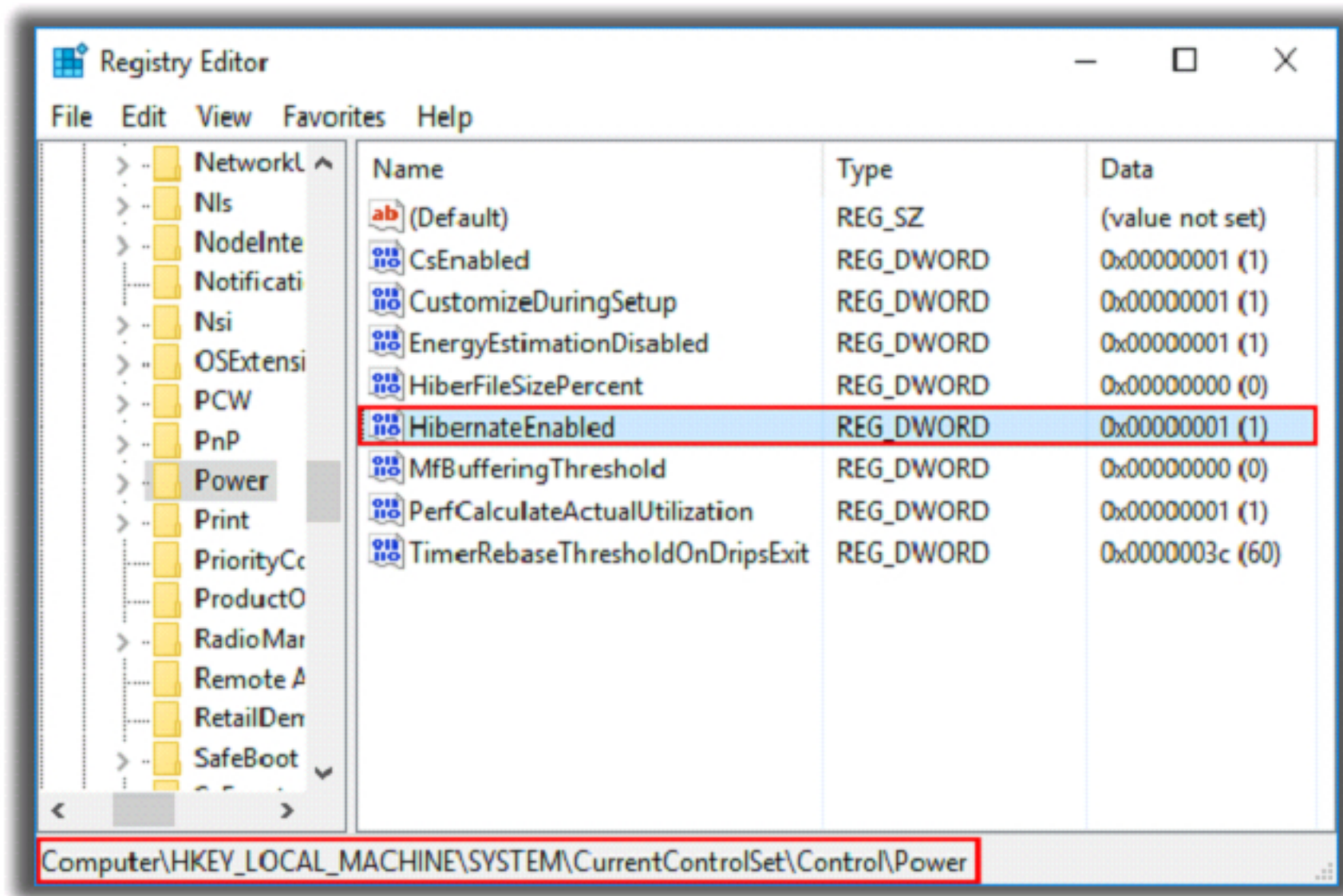




FIGURE 6.1: HibernationEnabled key in the Registry Editor

The system stores the hiberfil.sys file in the default folder as a hidden file, which occupies the size similar to that of available RAM space in the system. The investigators can select the file and use tools, such as Hex editor to analyze it.


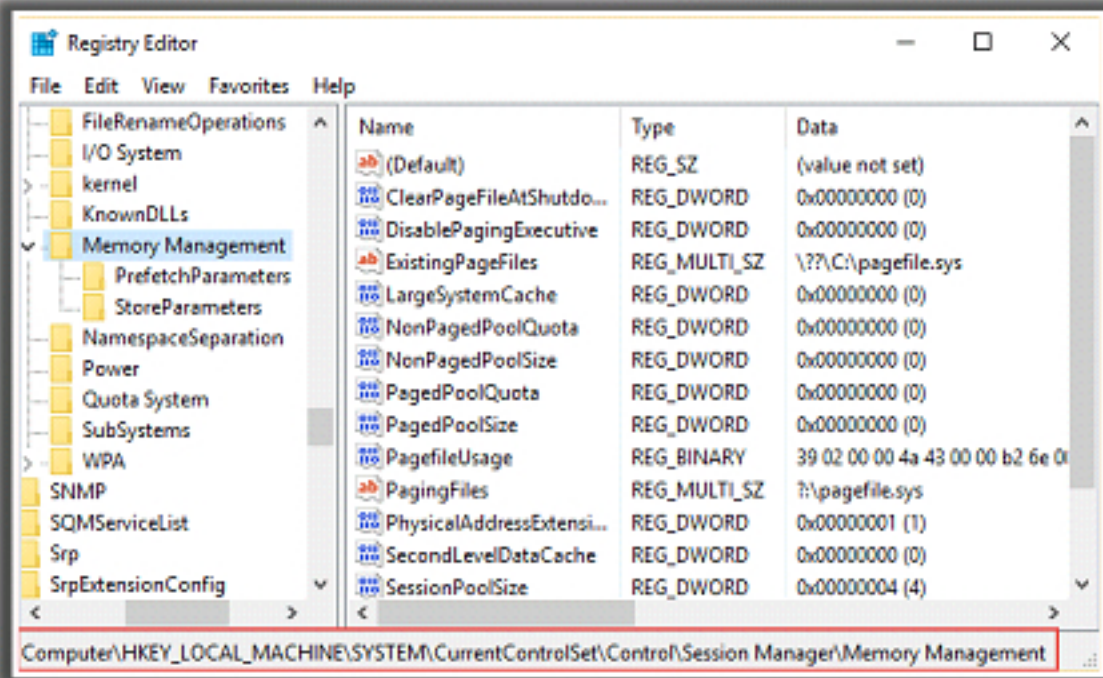

Page File



- Pagefile.sys is a **virtual memory** file used to expand the physical memory
- Stores **inactive processes** data and **sensitive data** such as User Ids, passwords, etc.
- Acts as a **swap file** to improve system performance



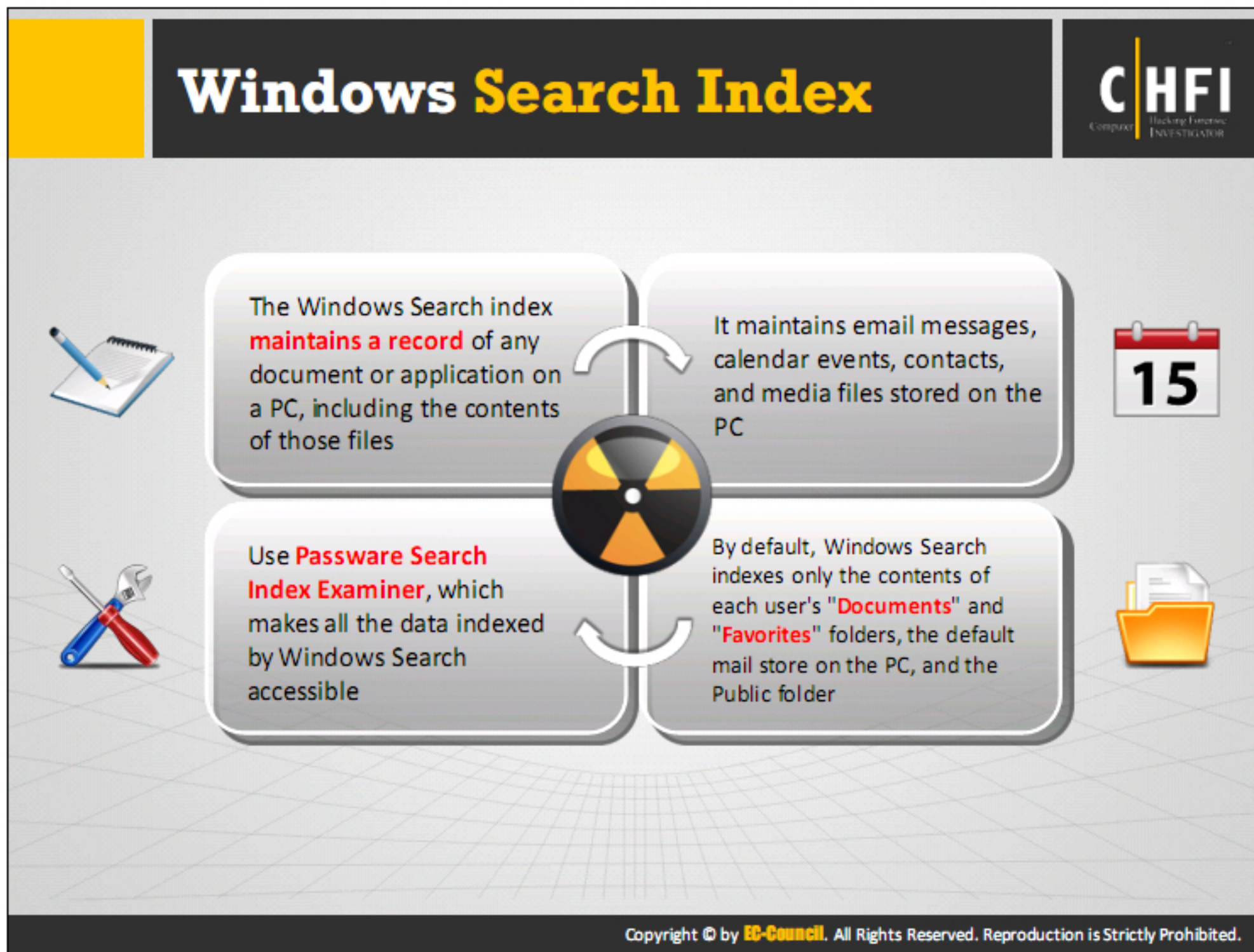
- Acquisition through special tools like rekall-master, Disk Explorer, Forensic Toolkit etc.
- The registry path for the page file is:
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pagefile.sys is a hidden file on the Windows operating system, which is used as virtual memory to expand the physical memory of a system. To increase the RAM performance the system moves the least used “pages” of memory into pagefile.sys file to free the RAM space and pools in the running applications.

Page file stores information about inactive processes, recently opened files and documents. It also accesses applications, as well as sensitive data such as User Ids, passwords, etc. used in the system processes. The system stores pagefile.sys file in the system drive folder as a hidden file. Investigators can extract it by navigating to the location or using software tools and analyze it using Hex editors.



Windows Search index supports indexing for over 200 common file types by maintaining a record of all the documents. It also allows the users to quickly access any document such as messages, calendar events, contacts, and media files.

Once the system index completes the initial scan of the PC, new files and email messages that arrive are indexed when the PC is idle—making the new files searchable shortly thereafter. After the initial scan, the system software updates the index continually, which can be used for monitoring the changes in the system.

Passware Search Index Examiner


Source: <http://www.lostpassword.com>

It makes all the data indexed by Windows Search accessible.

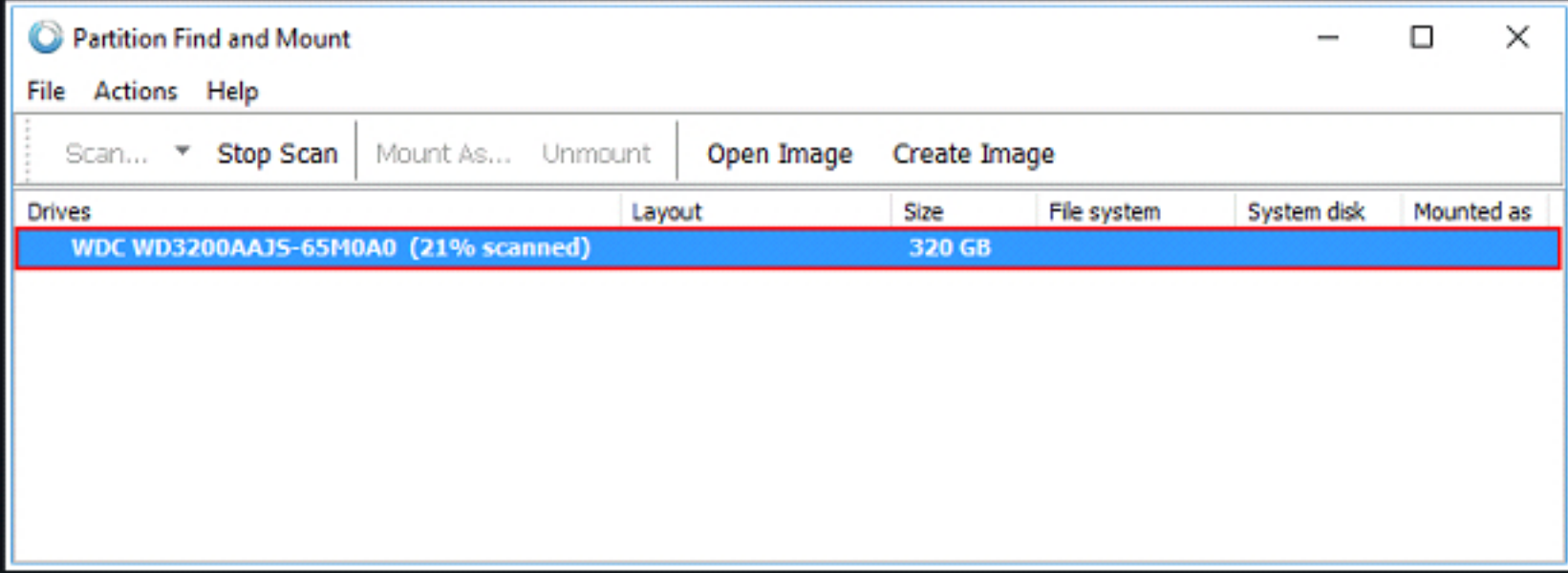
Key features include:

- Lists all the emails, documents, spreadsheets, and other items indexed by Windows Desktop Search
- Retrieves item properties, such as creation and modification dates, author, recipients, and summary content
- Requires only one file from the target PC, a Windows Desktop Search Database (.edb)
- Saves reports in common formats: XML, Comma Separated Values (.csv)

Collecting Hidden Partition Information



- Hidden partition is a **logical section of a disk** which is not accessible to the operating system
- Hidden partition may contain files, folders, confidential data, or backups of the system
- Tools like **find & mount** help to collect the information from the hidden partition
- Partition Logic can create, delete, erase, format, defragment, resize, copy, and move partitions and modify their attributes



The screenshot shows the Partition Find and Mount application window. It has a menu bar with File, Actions, and Help. Below the menu bar is a toolbar with buttons: Scan..., Stop Scan, Mount As..., Unmount, Open Image, and Create Image. The main area is a table with columns: Drives, Layout, Size, File system, System disk, and Mounted as. One row is highlighted in blue, showing 'WDC WD3200AAJS-65M0A0 (21% scanned)' with a size of '320 GB'. The URL 'http://findandmount.com' is visible at the bottom right of the window.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Partition Logic

Source: <http://partitionlogic.org.uk>


Partition Logic is a hard disk partitioning and data management tool. It can create, delete, erase, format, defragment, resize, copy, and move partitions and modify their attributes. It can copy entire hard disks from one to another.


Partition Find & Mount











Source: <http://findandmount.com>

Partition Find & Mount implements a new concept of deleted or lost partition recovery. It locates and mounts partitions into the system, thus making those lost partitions available. It will also work in case any Boot Record (including the Master Boot Record) is missing, damaged or overwritten.

Hidden ADS Streams





-  Alternate Data Stream (ADS) **NTFS** feature that helps to store **metadata** related to the location of a specific file 
-  Low on storage, remains hidden and helps attackers in installing rootkits and other malware 
-  ADS can be created by running a command like a **notepad** `visible.txt:hidden.txt` in command prompt 
-  Data can be copied into an ADS by using a command like `type a textfile > visible.txt:hidden2.txt` 
-  ADS information can be copied into a new file using a command like `more < visible.txt:hidden2.txt > newfile.txt` 


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The ADS or alternate data stream is a NTFS file system feature, which helps users to find a file using alternate metadata information such as author title. It allows the files to have more than one stream of data, which are invisible to the windows explorer and require special tools to view. The ADS offers ease in creating and accessing the additional streams, thus making it easy for the perpetrators to hide the data within the files and access them when required. Attackers can also store executable files in the ADS and execute them using the command line utility.


The ADS contains metadata including access timestamps, file attributes, etc. Investigators need to find the ADS and extract the information present in it. The system cannot modify the ADS data, thus retrieving ADS data can offer raw details of the file and execution of malware.

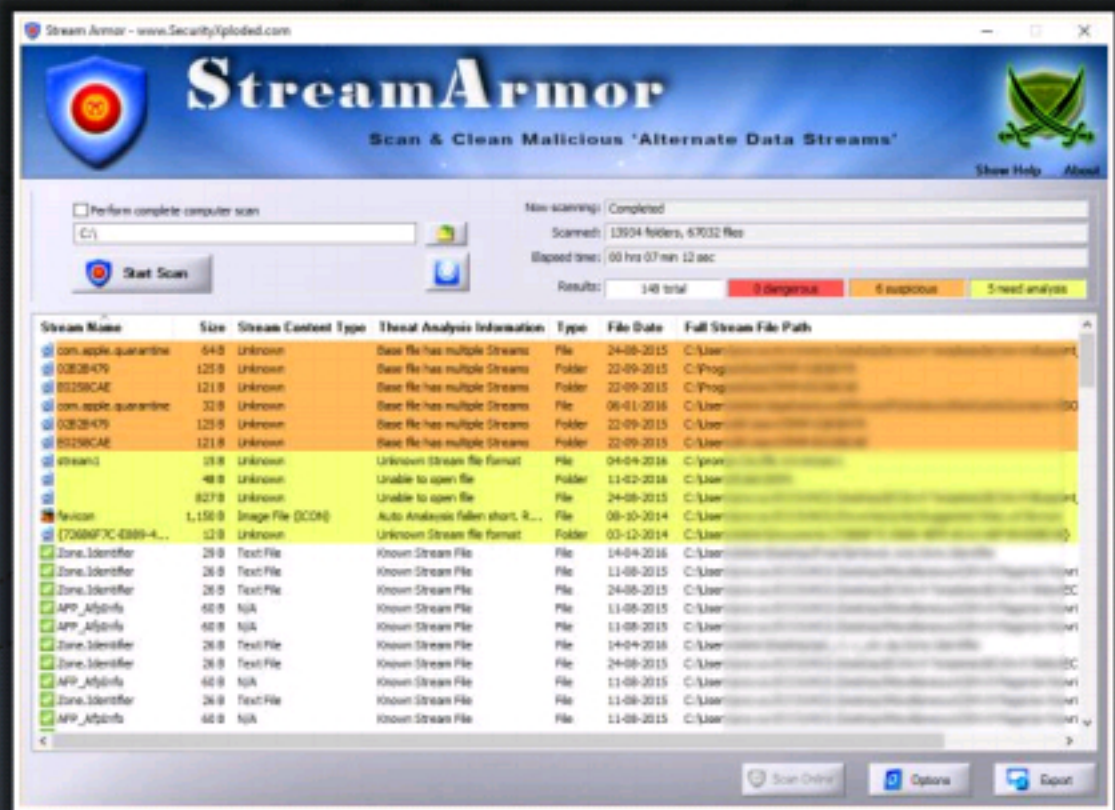
Apart from using the above mentioned methods, investigators can also use software tools to identify ADS files and extract the additional streams.

Investigating ADS Streams: StreamArmor



- StreamArmor **discovers** hidden alternate data streams (ADS) and cleanses them completely from the system.
- It comes with fast **multi threaded ADS scanner** which can recursively scan over the entire system and uncover all hidden streams.



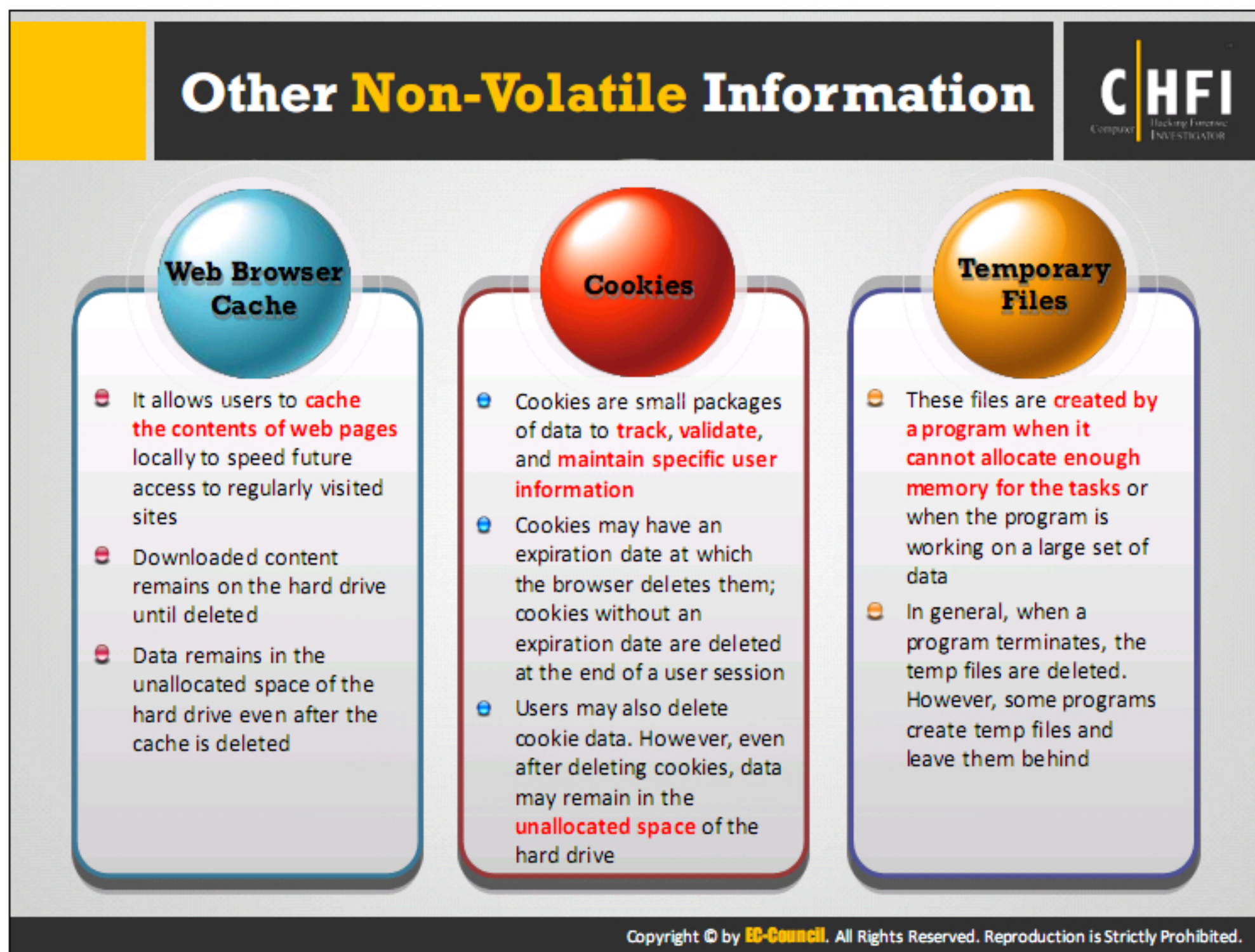


<http://securityxplored.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Stream Armor is the tool used to discover Hidden Alternate Data Streams (ADS) and clean them completely from system. In this tool, auto analysis is coupled with Online Threat Verification mechanism. It consists of a multi-threaded ADS scanner and a built in File Type Detection system.

Source: <http://securityxplored.com>



Web Browser Cache

The web browser cache allows users to cache the contents of web pages locally, in order to speed future access to regularly visited sites. This can be done because, the downloaded content remains on the hard drive until deleted. However, the data remains in the unallocated space of the hard drive even after deleting the cache.

ChromeCacheView

Source: <http://www.nirsoft.net>

ChromeCacheView is a small utility that reads the cache folder of Google Chrome Web browser, and displays the list of all the files that are currently stored in the cache. For each cache file, the following information is displayed: URL, Content type, File size, Last accessed time, Expiration time, Server name, Server response, etc.

Cookies

Cookies are small packages of data made to track, validate, and maintain specific user information. Cookies may have an expiration date, after which the browser deletes it. The system can also delete the cookies without the need of an expiration date at the end of a user session. The users may also delete cookie data directly from the browser. However, even after deleting cookies, the data may remain in the unallocated space of the hard drive. The cookies can store data in encrypted form, mostly in an index.dat file, which includes the date and time information. The investigators can use this file to fetch any evidence regarding the incident.

ChromeCookiesView


Source: <http://www.nirsoft.net>







ChromeCookiesView displays the list of all cookies stored by Google Chrome Web browser. It also allows deleting unwanted cookies and exporting the cookies into text/csv/html/xmlfile. For every cookie, the following information is displayed: Host Name, Path, Name, Value, Secure (Yes/No), HTTP Only Cookie (Yes/No), Last Accessed Time, Creation Time, Expiration Time.

Temporary Files

Programs and processes create temporary files when they cannot allocate enough memory for the tasks or when the program is working on a large set of data. In general, when a program terminates, the system deletes these temp files. However, some programs create temp files and leave them behind. These files contain information about all the system processes which can be useful to gather evidences in any forensic investigation.


Analyze the Windows Thumbcaches



- 
 - In Windows OS thumbnail images can be stored using a **thumbnail cache** for Windows Explorer thumbnail view
- 
 - This will **allow to open** these small **images quickly** and avoid Windows to create a new image always
- 
 - Thumbnail cache is mainly implemented to **avoid severe disk I/O, CPU processing, and load times** when every file in a folder needs to be opened as a thumbnail
- 
 - Windows XP had a **thumbs.db** file that stored the thumbnail image of every file
- 
 - This functionality was removed in Windows 7 and replaced the thumbs.db folder with a **thumbcache.db** file
- 
 - In Windows 10 thumbcache.db file stores the thumbnails in the same location as Windows 7: **C:\Users\<USERNAME>\AppData\Local\Microsoft\Windows\Explorer**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyze the Windows Thumbcaches (Cont'd)



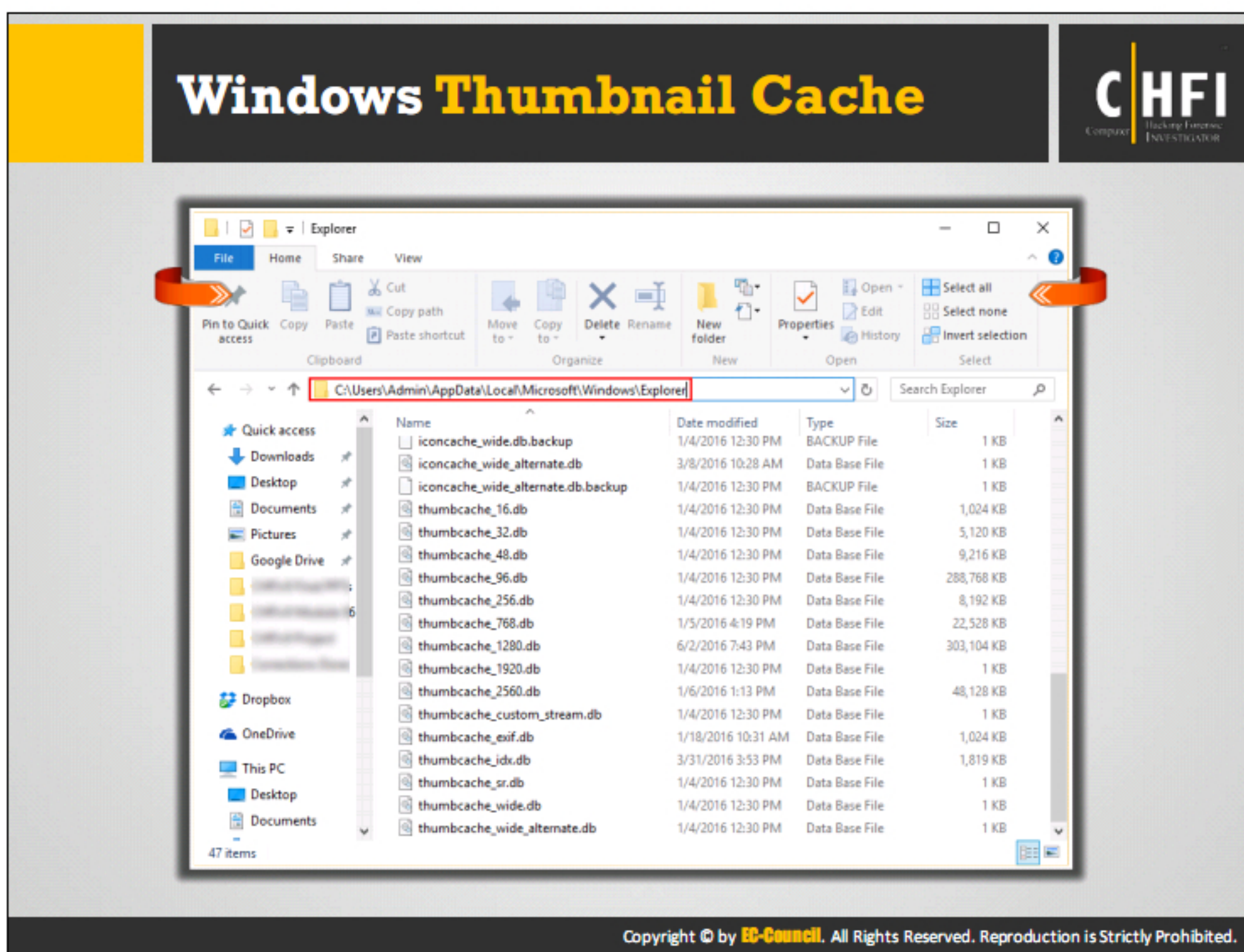
- Thumbnailcache analysis also helps to **find extra information about thumbnail pictures** and the original file used to create the thumbnail, like the original file name, the date each thumbnail was last written, etc.

- There are many tools to view and analyze thumbcache files e.g. **Encase, AccessData FTK, Thumbcache Viewer**, etc.

- Thumbcache Viewer allows extracting **thumbnail images** from the **thumbcache_*.db**

- This tool can be helpful in forensic analysis to know about the thumbnail cache details like **image names, the timestamps when they were saved, their locations**, etc.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Most operating systems use thumbnail feature to display images and other files on the folder for easy identification. Microsoft Windows OS use thumbnail cache to store thumbnail images that Windows Explorer use to produce the thumbnail view. The thumbnail cache will reduce the load on computer system by storing the smaller images in a single folder named thumbcache.db.

Images form strong evidences in various crimes, that's why suspects delete these images to avoid getting caught. It is because of the fact that the thumbnail of an image remains on a computer even after deleting the file itself. This helps the investigators to find if the suspect had deleted any files and it also gives a brief detail about the file that has been deleted.

Thumbcache Viewer


Thumbcache Viewer allows you to extract thumbnail images from the thumbcache_*.db and iconcache_*.db database files found on Windows Vista, Windows 7, Windows 8, Windows 8.1, and Windows 10. The program comes with both graphic user interface and command-line interface.

Source: <https://thumbcacheviewer.github.io>

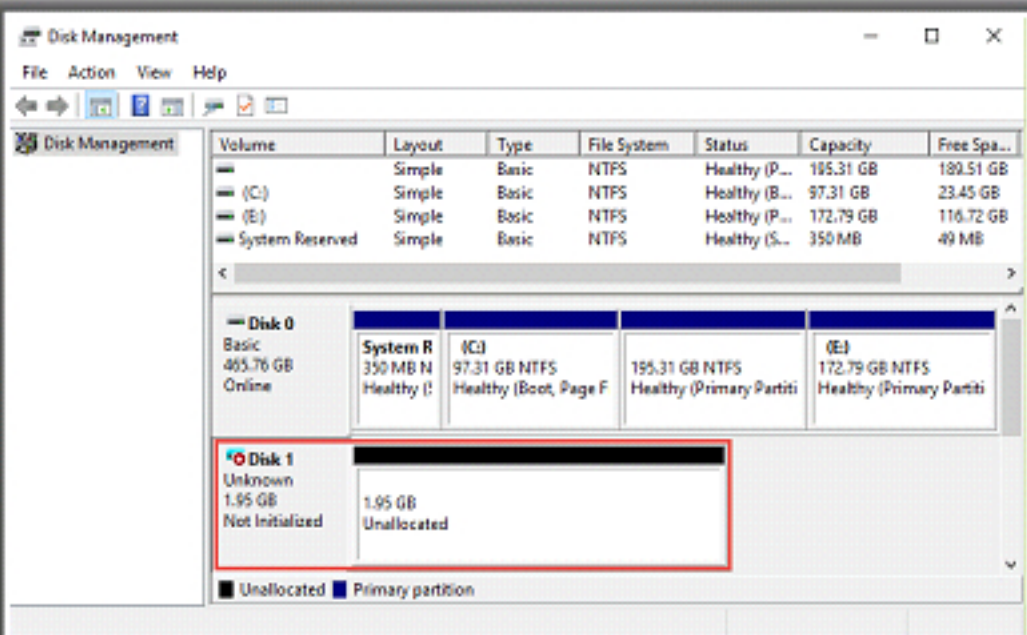


Memory of a system refers to the storage space, where the system saves important data required for processing, such as application files, virtual memory, etc. This space contains files and metadata required for functioning of the in-built and external applications. Investigators can analyze this space to find the installed application, recent events, and other related data.

Virtual Hard Disk (VHD)



- Virtual Hard Disk (VHD) is a file format that **stores data in a single file** and can be used as a hard disk for the virtual machine. '.vhd' is the file extension for VHD
- Data in a mounted VHD is **hard to track when un-mounted**, the data can be tracked only by vice-versa process or using specific tools
- The un-mounted disk can be opened by mounting and encrypting the .vhd file using **volume encryption tools**. BitLocker is another file encrypting algorithms
- The file can also be searched by sorting the **'vhd'** file extension in the user's image
- The investigator can check for the mounted VHD in Disk Management used by the suspects to **hide files**




Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

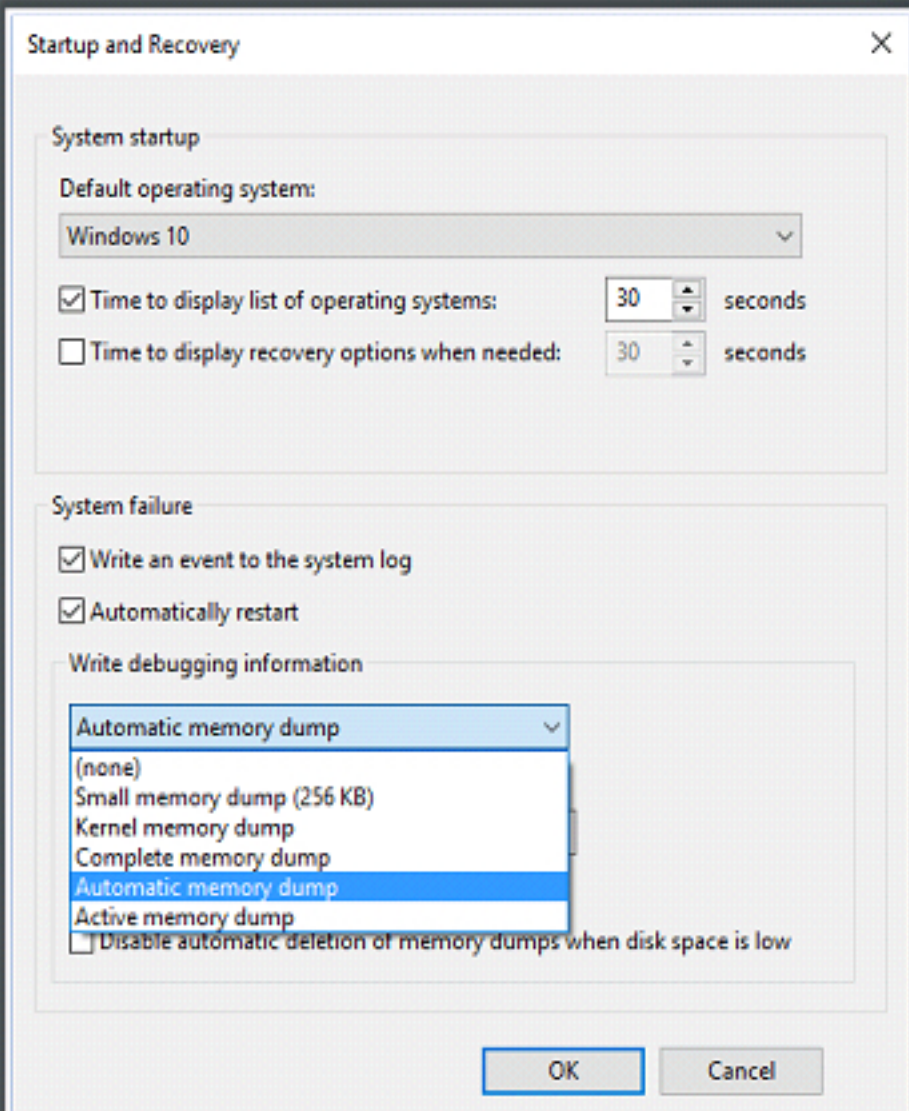
Virtual Hard disk is a disk image file format, which is having the functionalities similar to a typical hard drive. It stores contents including a file system, disk partitions, boot record, files, and folder.

Attackers use virtual drives to store malicious data. Data is readable only when the VHD is mounted; when un-mounted the contents of the VHD looks like a large unreadable file and the files are visible only through remounting. In such cases the forensic investigators use forensic tools to retrieve the information from the suspect virtual drives.

Memory Dump



- Memory dump (also known as crash dump) contained the contents of physical memory at the time the dump is created
- It is often used to diagnose a bug in a program, as programs create a memory dump when they halt unexpectedly
- It includes all the information regarding **stop messages**, a list of **loaded drivers**, and information about the processor that stopped
- The information in memory dumps is in binary, octal, or hexadecimal format
- You can check the memory dump information using **DumpChk** utility
- In Windows 10, the OS creates the following memory dumps:
 - Automatic memory dump
 - Complete memory dump
 - Kernel memory dump
 - Small memory dump



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory dump or crash dump is a storage space, where the system stores a memory backup, in case of a system failure. The system also creates a memory dump when it does not have enough memory for system operation. This backup enables users to examine the cause of the system crash and helps to know about any errors in the applications or in the operating system. In Windows systems it is also known as the blue screen of death (BSOD).

The core dump notifies about the system state, memory locations, application or program status, program counters etc. before the system failure. The system should reboot to be accessible after the memory dump. This memory also maintains a system log file for future reference.

The investigator can check the system for any memory dumps, in order to gather the system information available in them. This information can act as evidences if the malware has resulted in a system failure. Use tools such as DumpChk to analyze the memory dump in such cases.

Dumpchk

Source: <https://msdn.microsoft.com>

DumpChk (the Microsoft Crash Dump File Checker tool) is a program that performs a quick analysis of a crash dump file. This enables you to see summary information about what the dump file contains. If the dump file is corrupt in such a way that it cannot be opened by a debugger, DumpChk reveals the same to the investigator.


Syntax: DumpChk [-y SymbolPath] DumpFile

Parameters

-y SymbolPath: SymbolPath specifies where DumpChk is to search for symbols.

DumpFile: DumpFile specifies the crash dump file that is to be analyzed.

Memory Dump (Cont'd)



<h3>Automatic memory dump</h3> <ul style="list-style-type: none">Contains same information as the kernel memory dump, however, it differs from the later in the way that Windows sets the size of the system paging fileBy default, this dump file is written to %SystemRoot%\Memory.dmp	<h3>Complete memory dump</h3> <ul style="list-style-type: none">Largest kernel-mode dump file, that holds all of the physical memory used by WindowsBy default, it does not contain physical memory used by the platform firmwareBy default, this dump file is written to %SystemRoot%\Memory.dmp
<h3>Kernel memory dump</h3> <ul style="list-style-type: none">Contains complete memory in use by the kernel when there is a crashIncludes memory allocated to the Windows kernel, hardware abstraction level (HAL), kernel-mode drivers, and other kernel-mode programsIt does not include any unallocated or allocated memory to user-mode applicationsBy default, this dump file is written to %SystemRoot%\Memory.dmp	<h3>Small memory dump</h3> <ul style="list-style-type: none">Has a fixed size of 64KB and is much smaller than the kernel and automatic memory dumpsIt includes bug check message and parameters, blue-screen data, processor context (PRCB) for the processor, process information and kernel context (EPROCESS), thread information and kernel context (ETHREAD), kernel-mode call stack for the thread, and a list of loaded driversThis dump files list is maintained in %SystemRoot%\Minidump directory

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A memory dump file records information that helps to identify the reason of the unexpected system failure. It includes all the information regarding stop messages, the stopped processes, and a list of loaded drivers. It helps when the hard disk has limited space. The Dump Check utility helps to create and load the memory dump files. It should also be considered that memory dump errors such as the blue screen memory dump error can also occur due to hardware problems. Various memory dump files include:

Automatic Memory Dump

Automatic memory dump is the default memory dump created in Windows 8 and Windows Server 2012 R2, in order to support the System Managed page file configuration. It contains same information as the Kernel memory dump, but allows the SMSS process to reduce the page file to a smaller size than that of the existing RAM.

Complete Memory Dump

A complete memory dump is a record of the complete contents of the physical memory or RAM in the computer at the time of the system crash. The complete memory dump will usually contain data from the processes that were running when the system collected the dump.

Kernel memory dump

Kernel memory dump is created by default in the %systemroot% folder as a memory dump file whenever a machine has kernel faults. The kernel memory dump files created by Windows system are of intermediate size. They record only the kernel memory and the information


regarding troubleshooting. Kernel memory dump size varies and contains only kernel mode read or write pages that exist in the physical memory at the time of system crash.

Small Memory Dump

Small memory dump is a 64 KB dump containing the stop code and a list of all the loaded drivers and parameters. It records information that assists in identifying the cause of the unexpected system crash. Small memory dump files are stored in the %systemroot% folder by default.

Note: If the user has set the path to store the kernel memory dump or small memory dump, the path is visible in the Dump file text box in the Startup and Recovery window.

EProcess Structure



- Each process on a Windows system is represented as an executive process, or **EProcess** block
- An EProcess block is a **data structure** in which various **attributes of the process**, as well as pointers to a number of other attributes and data structures relating to the process, are maintained
- EProcess contents can be viewed with the help of the **Microsoft Debugging tools** and **liveKD.exe**
- dt -a -b -v _EPROCESS** command helps to see what the entire contents of an EProcess block looks like

Elements that are important to forensic investigation in the EProcess structure:

- PPEB_LDR_DATA** (pointer to the loader data) structure that includes pointers or references to modules (DLLs) used by the process
- A pointer to the image base address, where the **beginning of the executable image** file can be found
- A pointer to the process parameters structure, which itself maintains the DLL path, **the path to the executable image**, and the command line used to launch the process

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Each process on the Windows operating system is associated with an executive process or Eprocess block. It is the basic data structure that stores various attributes of the process and the pointer to the other attributes and data structures related to the process. The investigator can read this data structure. The data structure is essentially a sequence of bytes, with each sequence having a particular meaning. The size and even the values of the structures change not only between operating system versions but also between service packs of the same version of the operating system.

It is relatively easy to view the contents of the EProcess structure. First, download and install the Microsoft debugging tools and the correct symbols for operating system and service pack. Then download LiveKD.exe, copy it into the same directory as the debugging tools. Once this is done, open a command prompt, change to the directory where the debugging tool is installed, and type the following command:

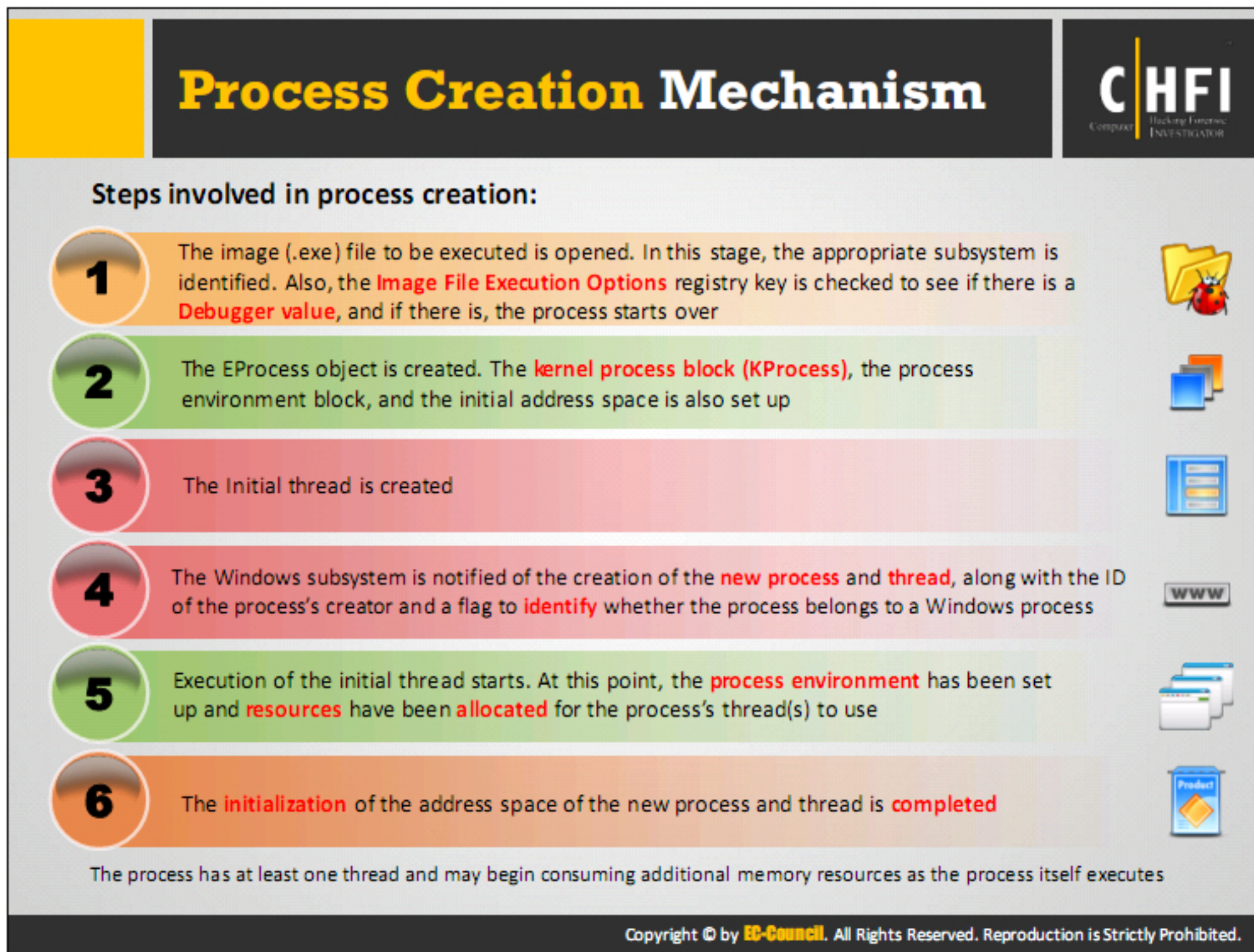
```
debug>livekd -w
```

This command will open WinDbg, the GUI interface to the debugger tools. To see the entire contents of an EProcess block, type **dt -a -b -v _EPROCESS** into the command window, and press Enter. The **-a** flag shows each array element on a new line, with its index. The **-b** switch displays blocks recursively. The **-v** flag creates a more verbose output, telling the overall size of each structure.

The process environment block, or PEB is an important element of all processes which is pointed to by the EProcess structure. This structure contains a great deal of information, but the elements that are important to forensic investigators are:

- A pointer to the loader data (referred to as PPEB_LDR_DATA) structure that includes pointers or references to modules (DLLs) used by the process.
- A pointer to the image base address where an investigator expects to find the beginning of the executable image file
- A pointer to the process parameter structure, which itself maintains the DLL path, the path to the executable image, and the command line used to launch the process


Parsing this information from a dump file can be useful to the investigator.





There are a number of steps that are followed when a process is created. These steps can be broken down into six stages:

1. The image (.exe) file to be executed is opened. During this stage, the appropriate subsystem (Posix, MS-DOS, Win 16, etc.) is identified, the Image File Execution Options registry key is checked to see if there is a debugger value, and if there is, the process starts over.
2. The EProcess object is created. The kernel process block (KProcess), the process environment block, and the initial address space are also set up.
3. The initial thread is created.
4. The Windows subsystem is notified of the creation of the new process and thread, along with the ID of the process' creator and a flag to identify whether the process belongs to a Windows process.
5. Execution of the initial thread starts. At this point, the process environment has been set up and resources have been allocated for the process's thread(s) to use.
6. The initialization of the address space is completed in the context of the new process and thread.

The process has at least one thread and may begin consuming additional memory resources as the process executes itself.



Parsing Memory Contents



Lsproc.pl:

- List Processes (Lsproc) locates processes
- It takes a single argument, the path and name to a RAM dump file
 - Ex: `c:\perl\memory>lsproc.pl d:\dumps\drfws1-mem.dmp`
- Output will be shown in six columns at the console

Proc	PPID	PID	Name of the process	Offset of the process structure within the dump file	Creation time of the process
------	------	-----	---------------------	--	------------------------------

Lspd.pl is a Perl script that allows a user to list the details of a process

Lspd relies on the output of **Lsproc** to obtain its information. **Lspd** takes two arguments:

- Path and name of the dump file
- Offset from the **lsproc.pl** output of the process

Ex: `c:\perl\memory>lspd.pl d:\dumps\drfws1-mem.dmp 0x0414dd60`

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The tools that parse memory contents usually employ the methodology of locating and enumerating the active process list using specific values/offsets (derived from system files) to identify the beginning of the list. Then the tools use the same methodology for walking through the double linked list, until all the active processes have been identified. The location of the offset for the beginning of the active process list was derived from one of the important system files, `ntoskrnl.exe`.

Lsproc.pl

Lsproc (short for list processes) locates processes but not threads. It takes single argument, the path, and name, to a RAM dump file:

Example: `c:\perl\memory>lsproc.pl d:\dumps\drfws1-mem.dmp`

The output of `lsproc.pl` appears at the console (i.e., STDOUT) in six columns.


Lspd.pl

Lspd.pl is a command-line Perl script that relies on the output of `lsproc.pl` to obtain its information. Specifically, `lspd.pl` takes two arguments: the path and name of the dump file and the offset from the `lsproc.pl` output of the process that the investigators are interested in. The command line to use `lspd.pl` is:


`c:\perl\memory>lspd.pl d:\dumps\drfws1-mem.dmp 0x0414dd60`

Lspd.pl also retrieves a list of the names of various modules (DLLs) used by the process and whatever available handles (file handles and so on) it can find in memory.

Parsing Process Memory




Use **strings.exe** or **grep** searches to parse through the contents of a RAM dump and look for interesting strings (passwords), IP or e-mail addresses, URLs, etc.




Lspm.pl takes the arguments, such as:

- Name and path of the dump file
- Physical offset within the file of the process structure



It extracts the available pages from the dump file and writes them to a file within the **current working directory**.

E.g.: `c:\perl\memory>lspm.pl d:\dumps\dfwrs1-mem.dmp 0x0414dd60`



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

In the past, investigators have used tools such as strings.exe or grep searches to parse through the contents of a RAM dump and look for interesting strings (passwords), IP or email addresses, URLs, etc. However, when investigators are parsing through a file which is about half a megabyte in size, there is not a great deal of context to the information.

Lspm.pl takes the same arguments as lspd.pl (the name and path of the dump file, and the physical offset within the file of the process structure) and extracts the available pages from the dump file, and writes them to a file within the current working directory. To run lspm.pl against the dd.exe process, use the following command line:

```
c:\perl\memory>lspm.pl d:\dumps\dfwrs1-mem.dmp 0x0414dd60
```

The output looks like this:


```
Name: dd.exe -> 0x01d9e000
```







```
There are 372 pages (1523712 bytes) to process.
```

```
Dumping process memory to dd.dmp...
```

```
Done.
```


Extracting the Process Image




-  **Lspi.pl** is a **Perl script** that takes the same arguments as **lspd.pl** and **lspm.pl**
-  It locates the beginning of the **executable image** for the process
-  If the Image Base Address Offset leads to an executable image file, **Lspi.pl** **parses the values** contained in the PE header to locate the pages that make up the rest of the executable image file
-  Example: **c:\perl\memory>lspi.pl d:\dumps\dfrrs1-mem.dmp 0x0414dd60**
-  **Reading Image Section Header Information** provides a road map that **Lspi.pl** uses to reassemble the executable image into a file
-  If successful, **Lspi.pl** writes the file out to the file based on the name of the process, with **.img** appended


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

When a process is launched, the executable file is read into memory. One of the pieces of information that can be obtained from the process details (via lspd.pl) is the offset within the dump file to the Image Base Address. Lspd.pl can do a quick check to see whether an executable image can be found in that location. To further develop this information, the PE file header can be parsed to see whether it is possible to extract the entire contents of the executable image from the dump file.

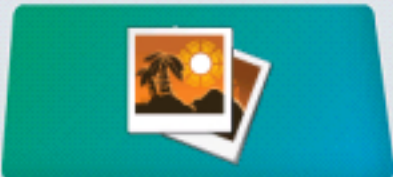
Extracting the Process Image (Cont'd)




Lspi.pl will not reassemble the file if any of the memory pages are marked as invalid and are no longer located in memory



Now, the extracted file from the memory dump will **not be exactly the same as the original executable file**, because some of the file's sections are writable, and those sections will change as the process is executing



As the process executes, various elements of the executable code (addresses, variables, etc.) will change according to the **environment** and the **stage of execution**



However, there are a couple of ways to determine the nature of a file and get information about its purpose:


- To see whether the file has **any file version information** compiled into it
- To use **file hashing** (Use a tool ssdeep that implements context-triggered piecewise hashing, or fuzzy hashing)

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Lspi.pl can't reassemble the file if any of the memory pages have been marked as invalid and are no longer located in memory. A file extracted from the memory dump will not be exactly the same as the original executable file. This is due to the fact that some of the file's sections are writeable, and those sections changes during the process execution step.

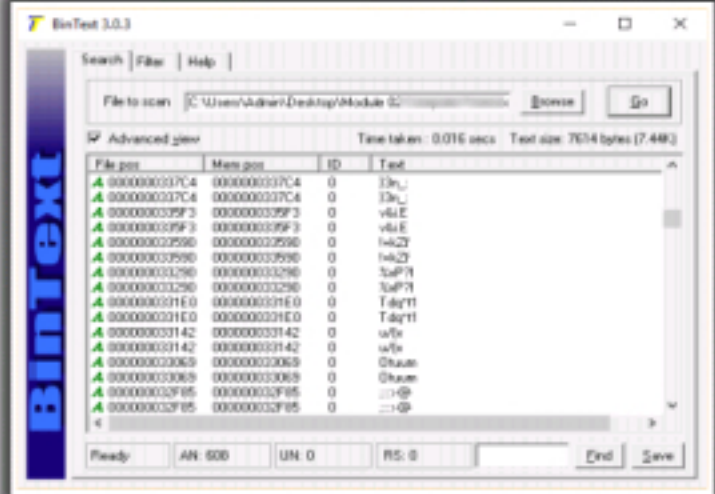
As the process executes, various elements of the executable code (addresses, variables, and so on) change based on the environment and the stage of execution. However, there are a couple of ways to determine the nature of a file and get some information about its purpose. One of those ways is to see whether the file has any file version information compiled into it, as is done with most files created by legitimate software companies. As noticed from the section headers of the image file, there is a section named .rsrc, which is the name often used for a resource section of a PE file. This section can contain a variety of resources, such as dialogs and version strings, and is organized like a file system. The file hashing option can also be used to get this information.

Collecting Process Memory



- Collect the contents of process memory available in a **RAM dump file**
- pmdump.exe** tool allows dumping the contents of process memory without stopping the process
- Process Dumper (pd.exe)** dumps the entire process space along with the additional metadata and the process environment to the console; it redirects the output to a file or a socket
- Userdump.exe** dumps any process without attaching a debugger and without terminating the process once the dump has been completed
- Another method of dumping a process is to use **adplus.vbs** script

- Once done with the dumping process, use **debugging tools** to analyze the dump files
- Other helpful tools include:
 - BinText**: Finds ASCII, Unicode and Resource strings in a file
 - Handle.exe**: Provides a list of handles that have been opened by the process
 - listdlls.exe**: Reports the DLLs loaded into processes



<http://www.mcafee.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

During an investigation, the investigator is usually interested in only particular processes rather than a list of all processes, and would like more than just the contents of process memory available in RAM dump file. For example, the investigator might have quickly identified processes of interest that required no additional extensive investigation.

There are ways to collect all the memory used by a process not just what is in physical memory but what is in virtual memory or the page file as well. The pmdump.exe tool allows dumping the contents of process memory without stopping the process. This allows the process to continue and the contents of memory to change while being written to a file, thereby creating a “smear” of process memory. Also, pmdump.exe does not create an output file that can be analyzed with the debugging tools.

Another method for dumping the contents of process memory is called Process Dumper. It dumps the entire process space along with additional metadata and the process environment to the console (STDOUT), so that the output can be redirected to a file or a socket.

Userdump.exe allows dumping of any process, without attaching a debugger and without terminating the process once the dump has been completed. Also, the dump file generated by userdump.exe can be read by the MS debugging tools. However, working of the userdump.exe command requires system installation of its specific driver.

Once done with the dumping process, use debugging tools to analyze the dump files. Other helpful tools include:

Volatility

Source: <http://www.volatilityfoundation.org>

The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile memory (RAM) samples. The extraction techniques are performed completely independent of the system being investigated but offers visibility into the runtime state of the system. The framework is intended to introduce people to the techniques and complexities associated with extracting digital artifacts from volatile memory samples and provide a platform for further work into this exciting area of research.

BinText

Source: <http://www.mcafee.com>

It can extract text from a file and find plain ASCII text, Unicode (double byte ANSI) text, and Resource strings, providing useful information for each item in the optional “advanced” view mode. Its comprehensive filtering helps prevent listing of unwanted. The gathered list can be searched and saved to a separate file as either a plain text file or in informative tabular format.

Handle

Source: <http://technet.microsoft.com>

Handle is a utility that displays information about open handles for any process in the system. You can use it to see the programs that have open files or to see the object types and names of all the handles of a program.

ListDLLs.exe

Source: <http://technet.microsoft.com>

It is a utility that reports the DLLs loaded into processes. It lists all DLLs loaded into all processes, or into a specific process. It can also list the processes that have a particular DLL loaded. ListDLLs can also display full version information for DLLs, including their digital signature, and it can be used to scan processes for unsigned DLLs.

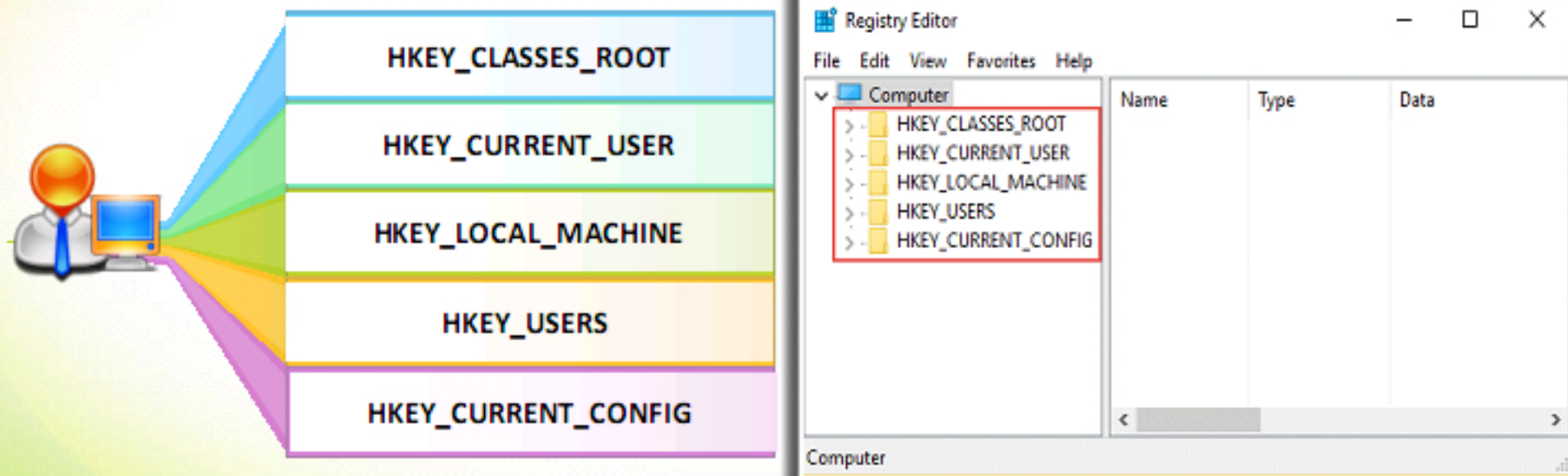


A Windows Registry contains potential information which is of evidential value and can support the forensic analysts in exploring the different aspects of forensic investigation. A forensic analysis in general is performed with a specific agenda in mind. In the forensic investigator's perspective, it is essential to know the type and significance of information to look for, and also where to find it. Forensic investigations which involve a windows platform vigorously require a careful assessment of the keys, sub keys and relevant values that are located inside the Windows registry. It is therefore crucial to understand and perform a Microsoft Windows Registry database analysis.

Inside the Registry



- An administrator can directly interact with the registry through any **intermediary application**, the most common are the **GUI registry editors** that come with Windows – **regedit** and **regedt32**
- There are **five root folders** in the Registry Editor:



Registry Editor view showing five root folders

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Inside the Registry (Cont'd)



Hives in the Windows registry play a critical role in the functioning of the system:

- 1 HKEY_USERS**
It contains all the actively loaded user profiles for that system
- 2 HKEY_CLASSES_ROOT**
This hive contains configuration information relating to which application is used to open various files on the system
- 3 HKEY_CURRENT_CONFIG**
This hive contains the hardware profile the system uses at startup
- 4 HKEY_LOCAL_MACHINE**
This hive contains a vast array of configuration information for the system, including hardware settings and software settings
- 5 HKEY_CURRENT_USER**
It is the active, loaded user profile for the currently logged-on user

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Inside the Registry (Cont'd)



The contents of much of the registry visible in the **Registry Editor** can be found in several files

Registry Path	File Path
HKEY_LOCAL_MACHINE\System	Windows\System32\config\SYSTEM
HKEY_LOCAL_MACHINE\SAM	Windows\System32\config\SAM
HKEY_LOCAL_MACHINE\Security	Windows\System32\config\SECURITY
HKEY_LOCAL_MACHINE\Software	Windows\System32\config\SOFTWARE
HKEY_USERS\Default	Windows\System32\config\DEFAULT

- Registry paths are volatile and do not exist in files on the **hard drive**
- These hives are created during **system startup** and are not available during **system shutdown**



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The Windows Registry is a hierarchical database that contains information, settings, system options, and other values about the system hardware, installed programs and profiles of the user accounts on the windows operating system.

The windows registry database stores information regarding the hardware attached to the system, the system options that have been selected, the computer memory that is setup and the application programs that are utilized when the operating system is running. The registry editor tool is used to view and edit setting in the system registry in a manual way. Normally it is not recommendable to make any changes in the system registry. The operating system makes the required updates in the registry automatically when needed.

The registry editor was used for the windows 3.1x, Windows 95 and later versions. The current version of Windows, Windows 10 uses RegEdit.exe as registry editor, whereas for Windows NT and earlier versions RegEdt32.exe served the purpose. However these tools do not reveal some of the registry metadata (for instance the last modified date).

There are five root folders in the Registry Editor:

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

HKEY_USERS

HKEY_USERS, abbreviated as "HKU", contains information about all the currently active user profiles on the computer. Each registry key under HKEY_USERS hive relates to a user on the computer, which is named after the user's security identifier (SID). The registry keys and registry values under each SID control the user specific mapped drives, installed printers, environmental variables and so on.

HKEY_CLASSES_ROOT

HKEY_CLASSES_ROOT, abbreviated as HKCR, is a sub-key of HKEY_LOCAL_MACHINE\Software. It contains file extension association information and also programmatic identifier (ProgID), Class ID (CLSID), and Interface ID (IID) data. This hive stores the necessary information which makes sure that the correct program opens when the user opens a file through the windows explorer.

HKEY_CURRENT_USER

HKEY_CURRENT_USER, abbreviated as HKCU, contains the configuration information related to the user currently logged on. This hive controls the user level settings associated with user profile such as desktop wall paper, screen colors, display settings etc.

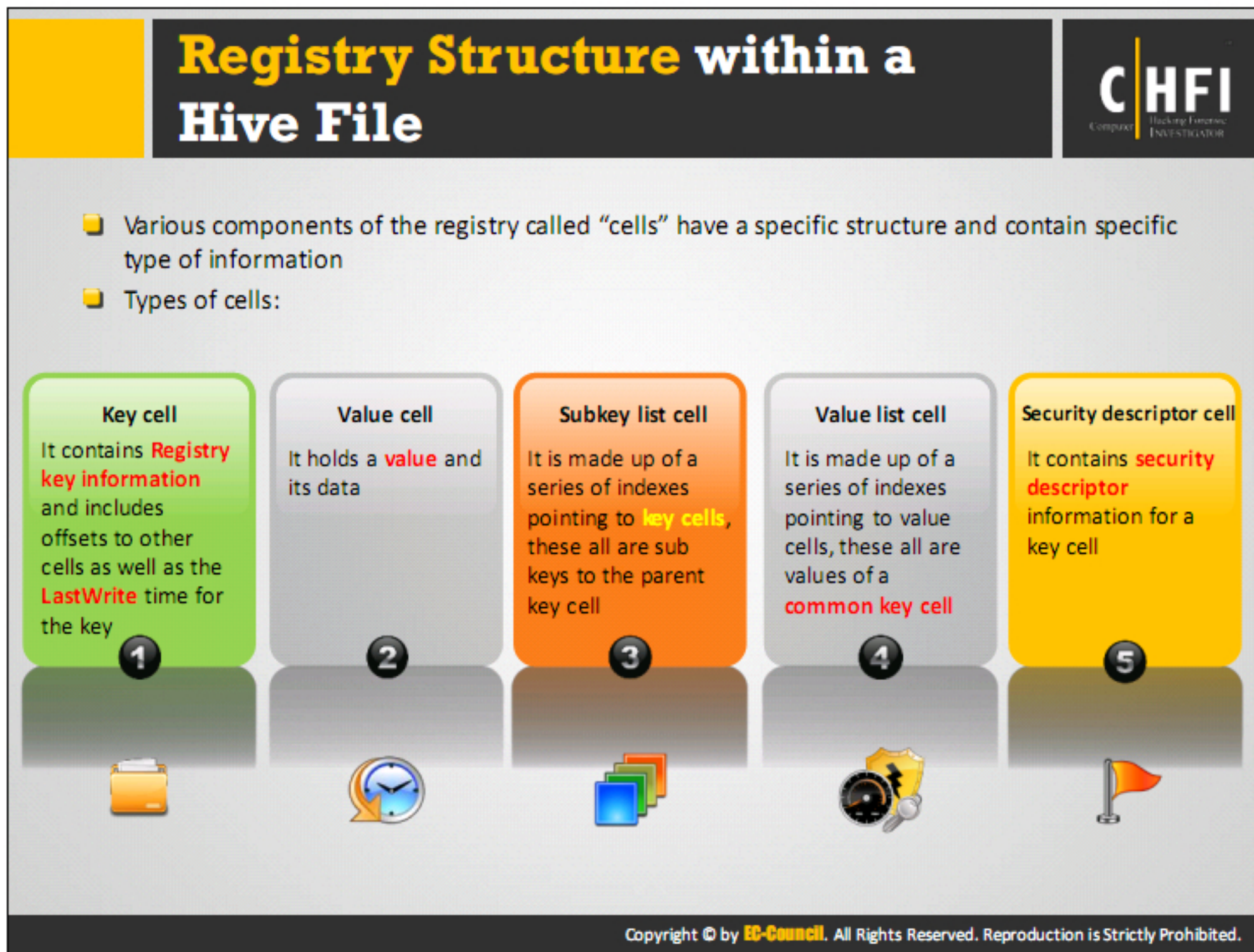
HKEY_CURRENT_CONFIG

HKEY_CURRENT_CONFIG, abbreviated as HKCC, stores information about the current hardware profile of the system. The information stored under this hive explains the differences between the current hardware configuration and the standard configuration.

The HKEY_CURRENT_CONFIG is simply a pointer to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\CurrentControlSet\Hardware Profiles\Current registry key, which contains the information about the standard hardware configuration that is stored under the Software and System keys.

HKEY_LOCAL_MACHINE

HKEY_LOCAL_MACHINE, abbreviated as HKLM, contains most of the configuration information for installed software which includes the Windows OS as well, and the information about the physical state of the computer which includes bus type, installed cards, memory type, startup control parameters and device drives.



It is essential for a forensic investigator to have a good understanding of the basic components of the registry. This will help them to glean extra information through keyword searches of other locations and sources that include the page file, physical memory, or even the unallocated spaces. By gaining more information about the registry structure, the forensic investigator can have a better understanding of what is possible and how to proceed further.

The registry component cells have a specific structure and hold specific types of information. The different types of cells are:

- Key cell
- Value cell
- Subkey list cell
- Value list cell
- Security descriptor cell

The Registry as a Log File



01

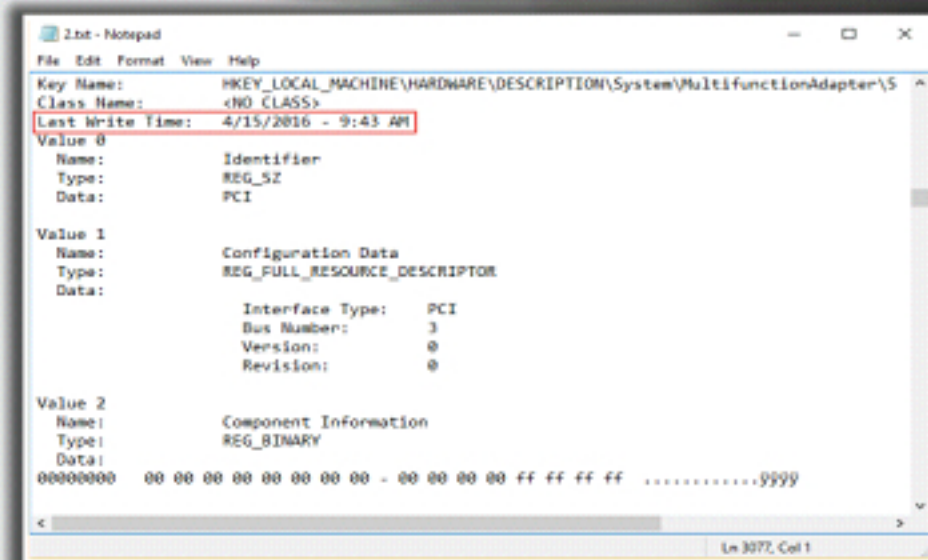
Registry is compared to the log file as it has some **action or event** associated with a **time**

02

LastWrite time is the property associated with **registry keys** similar to the **last modification time** associated with files and directories

03


This information provides a **timeframe reference** for certain user activities on the system, and it also tells when a **specific value** was added to a key or modified



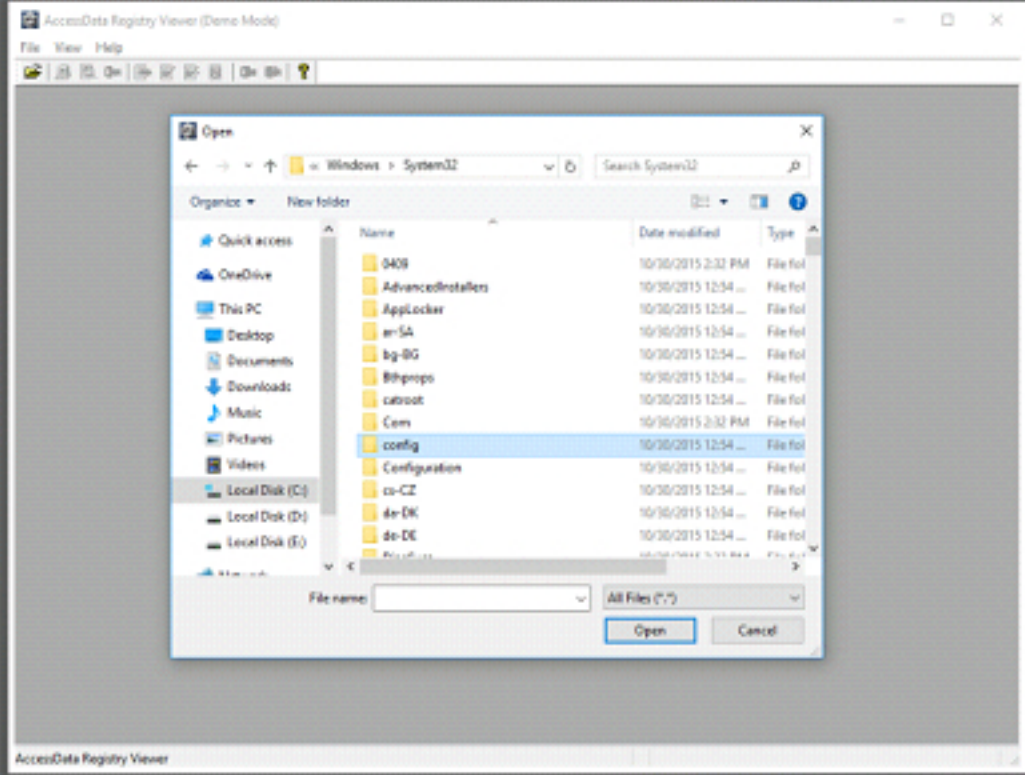
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Each registry key in a Windows Registry holds a time stamp embedded inside them which is referred to as the Last Write Time. This is comparable to that of the last modified time for a file. At any point of time when the registry key or any of its values are created, altered, or deleted the value is updated to the current local system time. Even though the registry value is not associated with any Last Write Time it can be inferred from the Last Write Time of a registry key.

Registry Analysis



- During a live response, much of the information **retrieved and analyzed** within the registry, and the complete data during **post-mortem investigation**
- ProDiscover tool can be used to access the **registry during postmortem analysis**
- Steps to obtain information using ProDiscover:
 - Load the case into ProDiscover
 - Right-click the **Windows** directory in the **Content View**
 - Choose **Add to Registry Viewer**
 - AccessData Registry Viewer locates files and displays them on the Registry Viewer



<http://accessdata.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

ProDiscover

The ARC Group ProDiscover® Basic edition is a self-managed tool for the examination of the user's hard disk security. ProDiscover Basic is designed to operate under the National Institute of Standards' Disk Imaging Tool Specification 3.1.6. It is made to collect snapshots of activities that are critical for taking proactive steps in protecting the user data. ProDiscover Basic has a built-in reporting tool to present findings as evidence for legal proceedings. The user can gather time zone data, drive information, Internet activity, and more, piece by piece, or in a full report as needed. The user has robust search capabilities for capturing unique data, filenames and file types, data patterns, date ranges, etc. ProDiscover Basic gives clients the autonomy they desire while managing their own data security.

RegRipper

RegRipper is a flexible open source tool that facilitates registry analysis with ease. It contains pre-written Perl scripts for the purpose of fetching frequently needed information during an investigation involving a Windows box. RegRipper is used because of its simplicity and also the easy availability of numerous plugins that capture specific information from the registry.

System Information

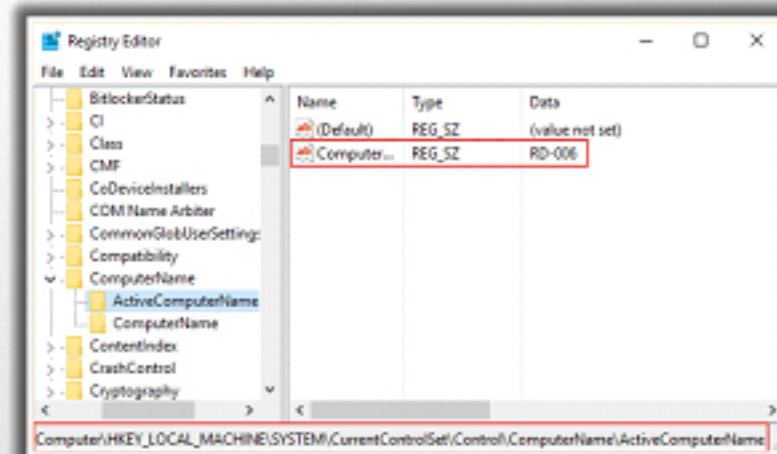
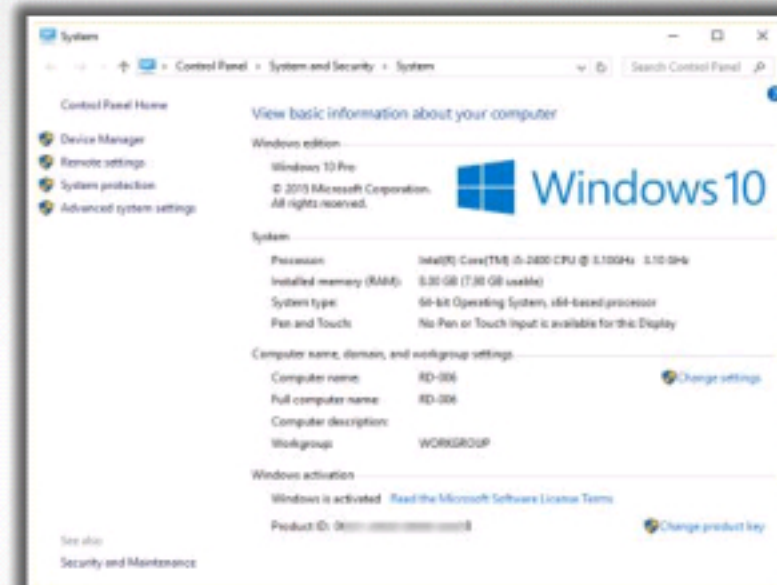
CHFI
Computer Hacking Forensic Investigator

- Click the **File Explorer** shortcut on the Taskbar to open **This PC** window, now right-click and choose **Properties** to see system information such as OS version, service pack level, computer name, etc.

- Other information about the system is stored in the **CurrentControlSet**, a volatile portion of the registry

- Find the computer name in the following key, in the **ComputerName** value:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName



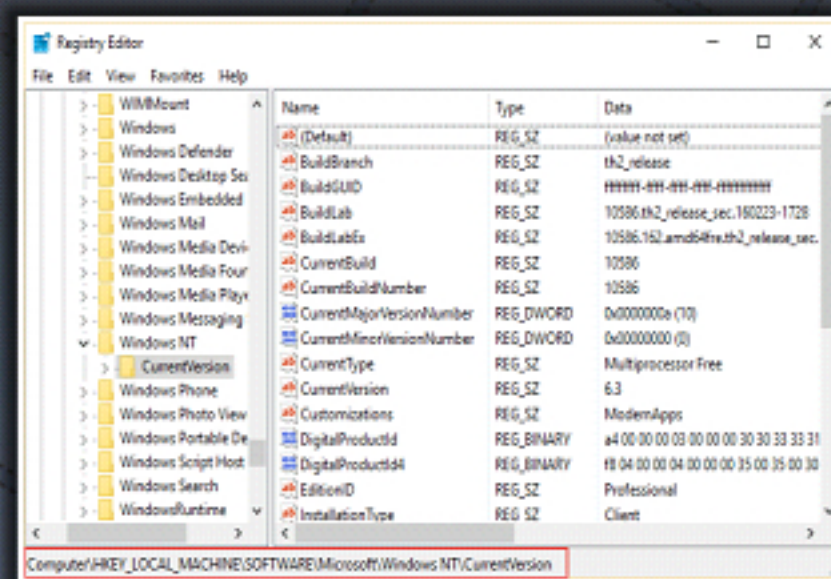
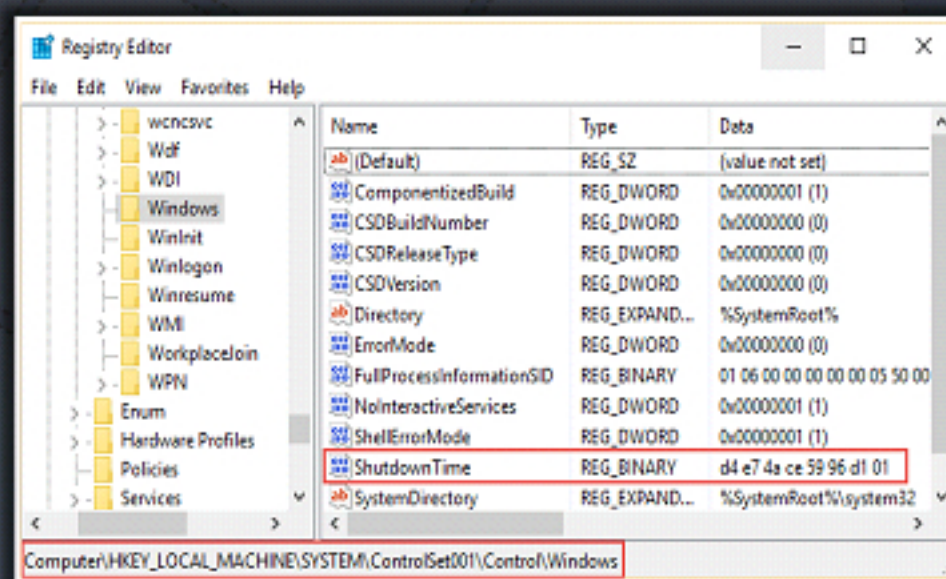
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

System Information (Cont'd)

CHFI
Computer Hacking Forensic Investigator

- Find the time when the system was last shut down in the following key:
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Windows

- Find the ProductName, CurrentBuildNumber, and CSDVersion in the following key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

While performing a postmortem analysis based on acquired image of a windows system, there is ample information available to the investigator. Majority of this information including the basic system information is easy to obtain during a live response, for instance the version of the operating system (like Windows 10, Windows 8, Windows 7 or Windows Vista) by just observing the shell. The keys for finding the computer name, the last shut down time, the product names; current build number and CSD version are listed in the slide.

Basically the system information is stored in the System and Software database files, and partially in the Security hive file. The information about the system users is stored in the Security Account Manager (SAM) database file. Each user's registry settings for their specific account is stored in the NTUSER.DAT registry file.

While downloading the RegRipper tool, the plugins also downloaded automatically with in the template files. This template file incorporates code for determining the current control set from a System hive file. The plugins within the /plugins directory help in deriving the information present in the System and Software hives.

The compname.pl plugin returns computer's name in the ComputerName value using the given key in the slide.

The winnt_cv.pl plugin returns ProductName, CurrentBuildNumber, and CSDVersion values using the given key in the slide, which give the details of the operating system and version. It also returns RegisteredOrganization, RegisteredOwner values, ProductId and InstallDate values, which help in further identification of the system.

TimeZone Information



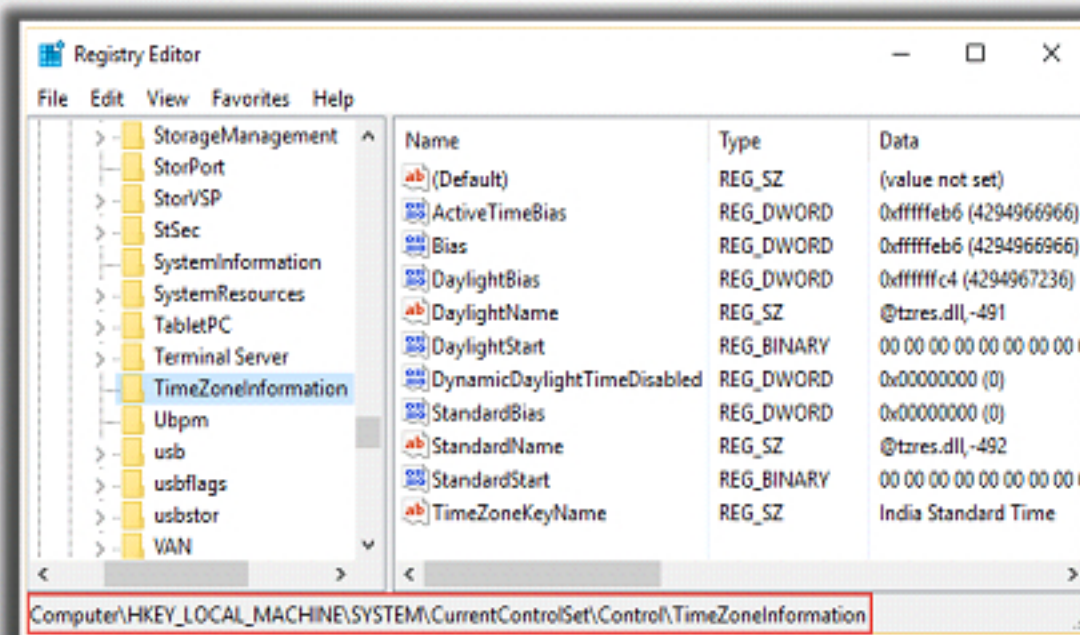
Find information about the time zone settings in the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation



This information can be important for establishing a activity timeline on the system

Use the **ActiveTimeBias** value from the **TimeZoneInformation** key to translate or normalize the times to other sources from the system, such as entries in log files



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

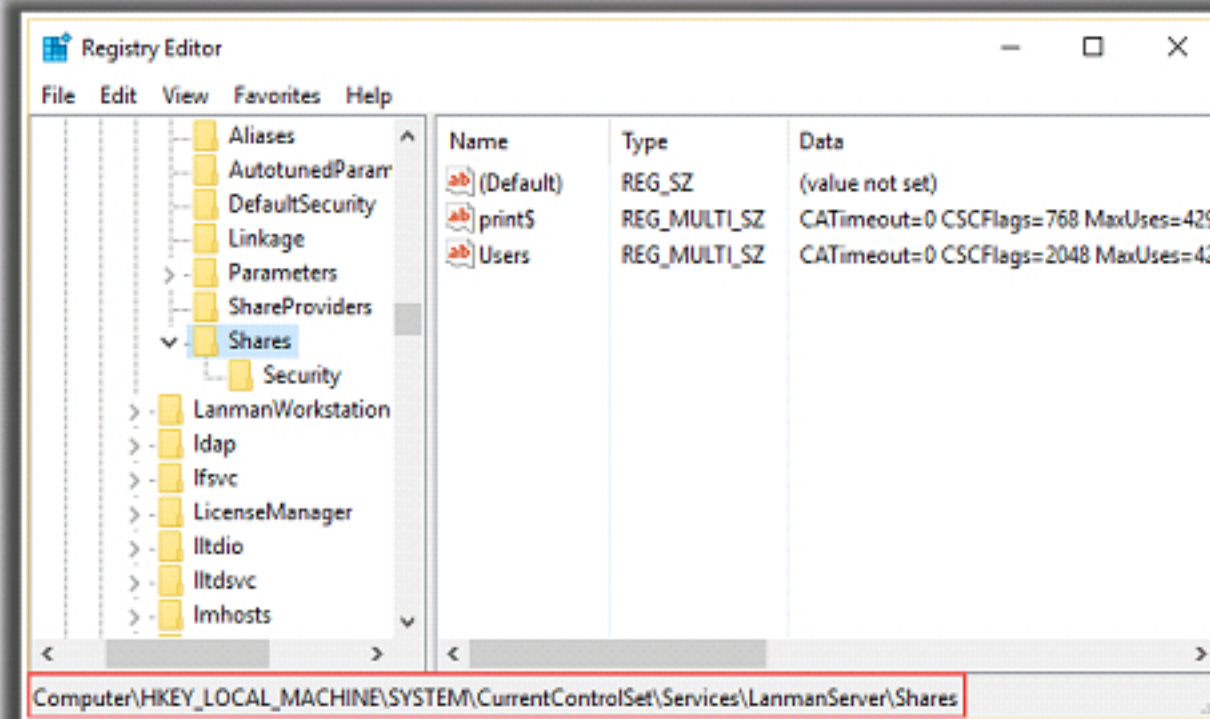
All the time zones installed on the system are present in the registry hive. The required key to find the information about the time zone settings is listed in the slide. Every time zone has its own unique key under the registry.

RegRipper's timezone.pl plugin returns the information about the time zone settings.

Shares



- Windows Vista, 7, 8.1, and 10 create hidden administrative shares on a system, by default
- If a user creates an additional share, such as via the **net share** command, that share will appear in the following key located in the **HKEY_LOCAL_MACHINE** hive:
SYSTEM\CurrentControlSet\Services\LanmanServer\Shares



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

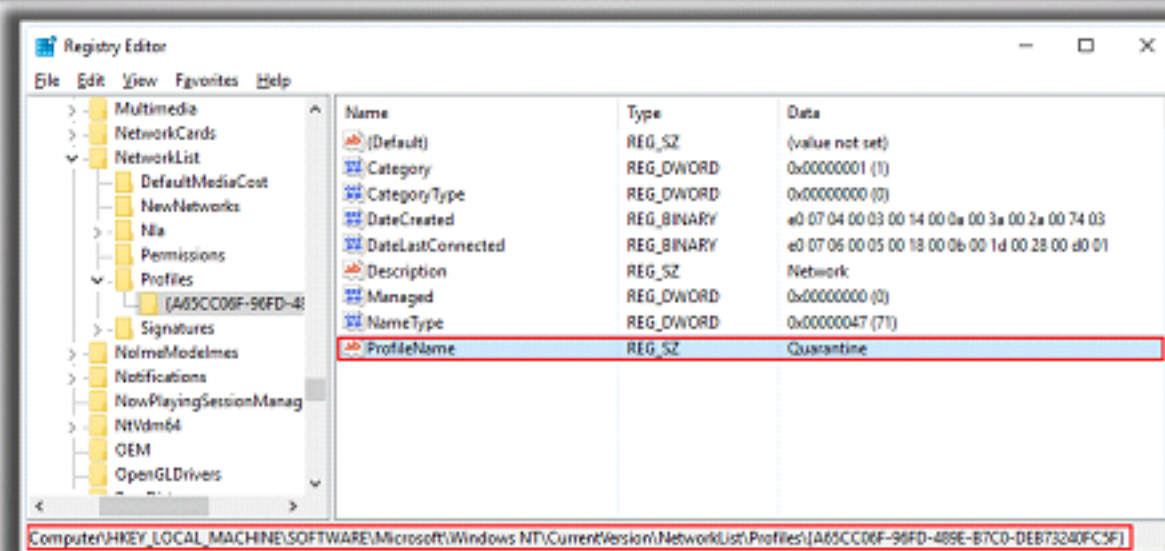
Often, Windows systems have share open for the users, so that they can access the system remotely. In many cases, this is valid for file servers; however, it might likewise be valid for user workstations, laptops, etc.

The shares.pl plugin returns information about available shares from a System hive file.

Wireless SSIDs



- On live systems, Windows 10 maintains a list of connected Wireless Service Set Identifiers (SSIDs)
- This list is maintained in the registry key:
 - SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{GUID}**
- Below this key, you might see a value **Active Settings** and other values called **Static#000x**, where x is an integer starting at 0
- These values are all binary, and SSIDs for any wireless access points that have been accessed will be included within the binary data
- The SSID name immediately follows this **DWORD** value for the number of bytes/characters listed



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Service Set Identifier, abbreviated as “SSID”, is a unique identifier that is used for naming a wireless local area network (WLAN). It consists of a sequence of 32 alphanumeric characters and is attached to the packets that are sent over a WLAN network. An SSID is also referred to as a “Network Name”. This name makes sure that data is sent to the correct destination when multiple independent networks are operating in the same physical location.

Wireless network configuration settings are stored within the windows registry, which includes SSIDs of networks that the system is connected to, network configuration parameters of those networks, and information about the Network Interface Cards on the system.


When a registry analysis is performed on a Windows XP system using the RegRipper tool, the tool captures the data in a text file, along with the information regarding the location of the keys. The Windows XP registry entries for wireless network connections are stored in the following location:

HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\{GUID}

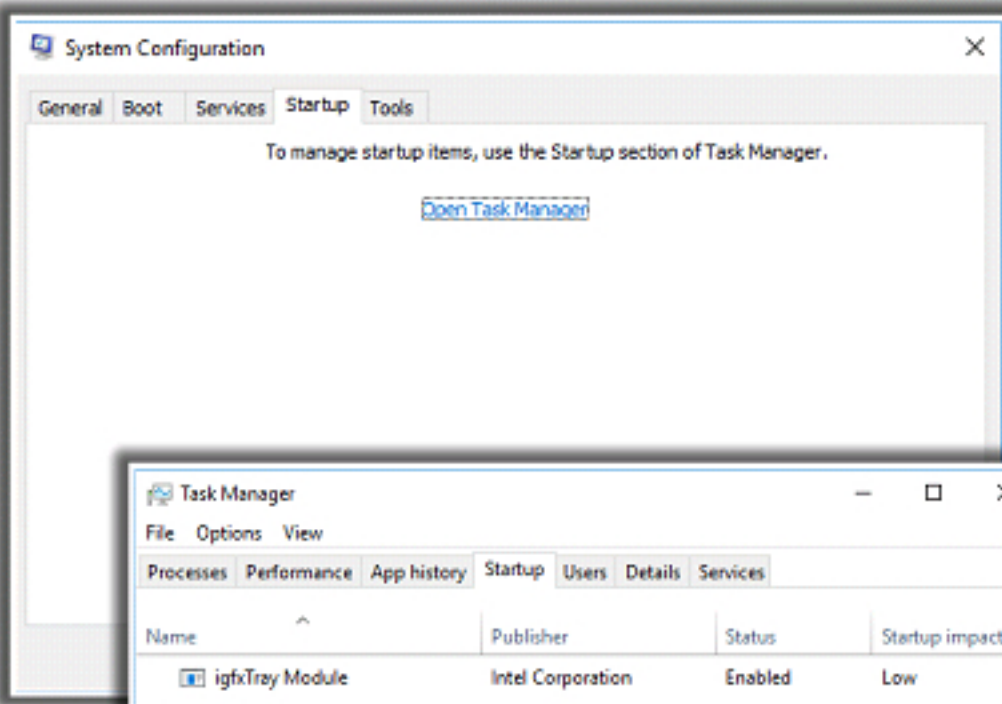
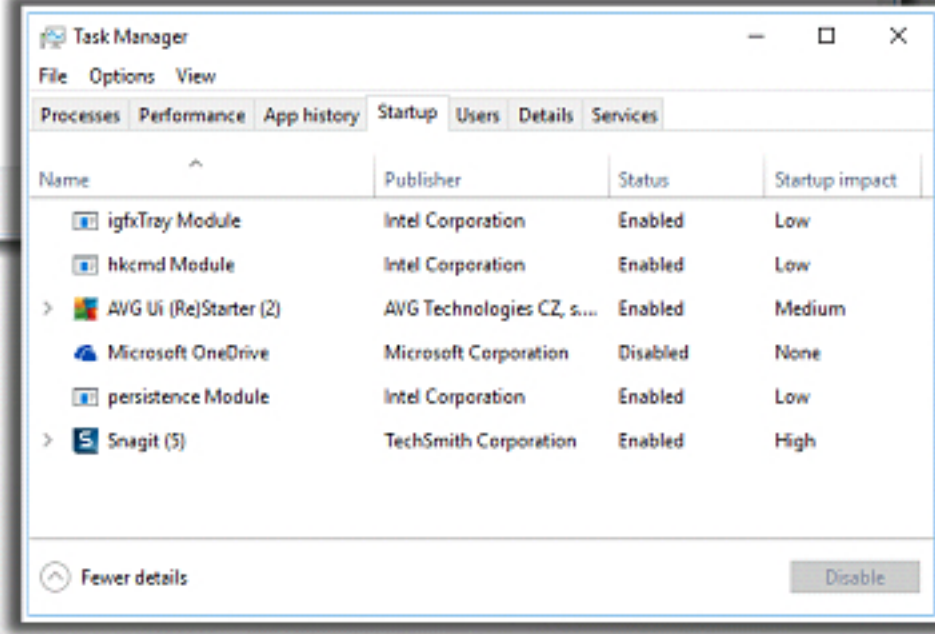
The picture in the slide represents an example of the above discussed registry. We can notice here that inside this registry there is some valuable information in different locations. Firstly, the ActiveSettings key contains the information for the active wireless profile on the system. When this key is selected, the SSID of the network is displayed. The picture represents an example of a network SSID shown in the slide.

Similarly, we can find more valuable information in the keys Controlflag and LayoutVersion.

Startup Locations



- Startup locations within the registry are locations that allow applications to be launched without any interaction from the user
- On a live Windows 10 system, the **msconfig** command launches the **System Configuration Utility**
- Path for the autostart option:
Start → type Run → press Enter → type msconfig → press Enter
- System Configuration window appears, select the **Startup** tab and click **Open Task Manager**
- **Task Manager** window appears displaying the **Startup** applications
- Alternatively, you may right-click on **Taskbar** and select **Task Manager**
- In the Task Manager window, click **Startup** tab


Name	Publisher	Status	Startup impact
igfxTray Module	Intel Corporation	Enabled	Low
hkcmd Module	Intel Corporation	Enabled	Low
> AVG Ui (Re)Starter (2)	AVG Technologies CZ, s.r.o.	Enabled	Medium
Microsoft OneDrive	Microsoft Corporation	Disabled	None
persistence Module	Intel Corporation	Enabled	Low
> Snagit (5)	TechSmith Corporation	Enabled	High

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Startup locations are folder locations within the registry that allows applications to launch automatically without any intervention made by the user. Some applications, such as touch pad drivers and applications on laptops, as well as antivirus and firewall applications, are most useful when they are started automatically.


However, in some cases there are programs that are not legitimate, like Trojans, worms, spyware, viruses where attackers use the autostart locations to automatically run these malwares when the system boots and thereby corrupt the system. Therefore, it is subsequently essential to regularly check the startup registry keys in the System Configuration utility and delete the unwanted keys.

Importance of Volume Shadow Copy Services



- Volume shadow copy is a Windows feature which **creates and maintains snapshots of the disk volumes**
- Block level snapshots** of any alterations on the system are generated
- The snapshots are called **shadow copies**
- These copies are scanned using forensic tools like **Internet Evidence Finder (IEF)** and investigators can analyze a specific copy of interest to find evidence

- Shadow copies will have the following information
 - a historical version of the registry hives
 - databases such as SQLite
 - several other artifacts
- To find extra data there are tools like **IEF Report Viewer** that give the investigator with details about the shadow copy and file the data fragment came from




Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Volume Shadow Copy Service-based backup (VSS) introduced in Microsoft Windows, allows the users to take backup copies of computer files or the logical drive even when the files are still in use. These backup copies are also referred to as shadow copies. This technology works with NTFS file system to generate and save the shadow copies.

The main importance of the volume shadow copy service is to create breakup of the data even when the application data is still running, which infers that the data files are open or in an instable condition. To do so, there has to be a proper coordination between the backup applications, and the system hardware and software components of the computer. The VSS technology facilitates this by providing proper conversation among the mentioned components. If all the components are in coordination with the VSS, the user can take the backup snapshots even without the application going offline.

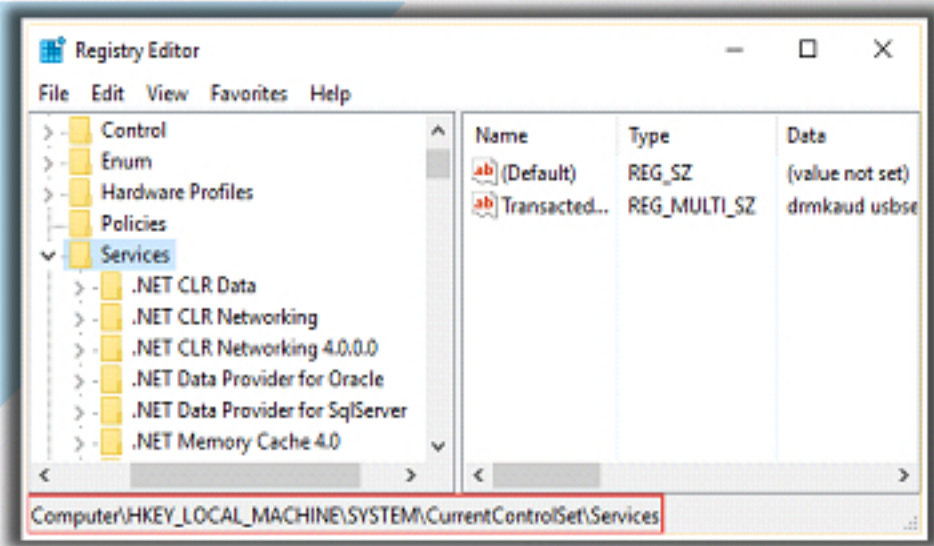
System Boot



- Malware can be launched within the **autostart locations** of the Registry during the system boots, even without user-intervention
- Example: Windows service at **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services**

- **Intrusion analysis** can be performed using ProDiscover, which locates the **ControlSet** marked **Current** and then sort the subkeys below the **Services** key based on their **LastWrite** times
- If there is any **mismatch** between the **LastWrite** times and the actual time that the administrator launched legitimate programs, it implies that there is a possible intrusion

- When the system starts, value of the **CurrentControlSet** to be used is determined and the settings for that **ControlSet** are used
- Services listed in the **ControlSet** are scanned and services that are set to start automatically are launched



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers are most likely to use the auto-start locations to automatically run the malwares when the system boots without the involvement of the user. An example of such auto-start location is given in the slide.

User Login



User Login

When a user logs into a system, the following **Registry keys** are accessed and parsed so that the listed applications can be executed:



- HKEY_LOCAL_MACHINE\ SOFTWARE \Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE \ Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software \Microsoft\Windows\CurrentVersion\RunOnce

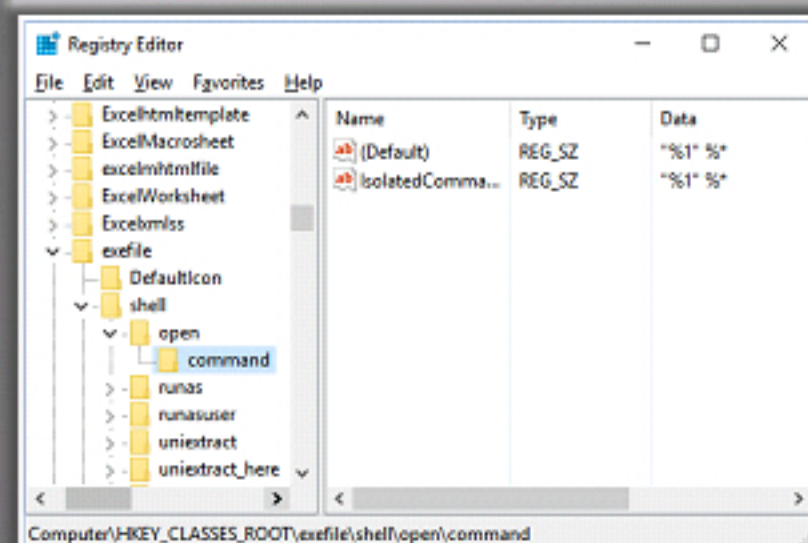
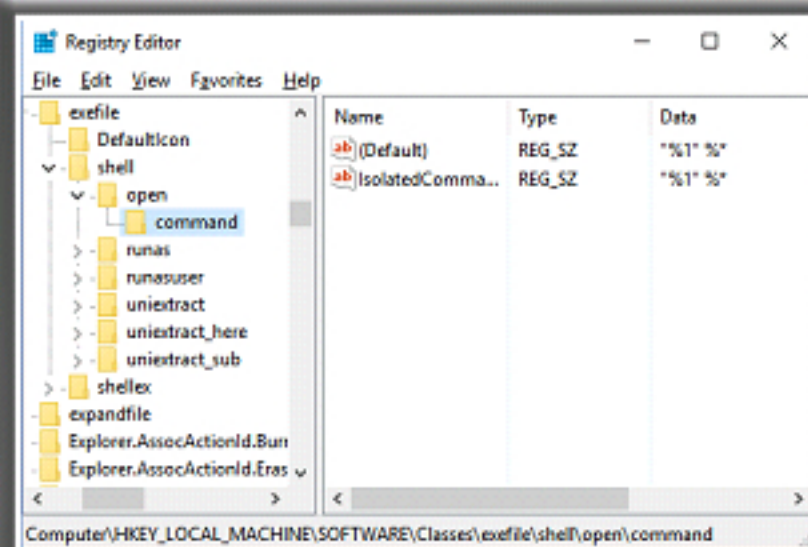
Note: These keys are ignored if the system is started in Safe Mode.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

User Activity




- Autostart Registry locations are accessed when the user performs any action, such as opening an application like **Outlook or Microsoft Edge**
- Look for malware in these locations:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command
 - HKEY_CLASSES_ROOT\exefile\shell\open\command
- Windows OS provides the ability to alert external functions when certain events occur on the system, such as a user logs on or off or the screensaver starts
- These notifications are handled by the Registry key:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
- Sort the sub-keys beneath **Notify** based on their **LastWrite** times and pay attention to the entries near to the date of the suspected incident
- Check for the entries that list DLLs in the **DLLName** value that have suspicious file version information or no file version information at all

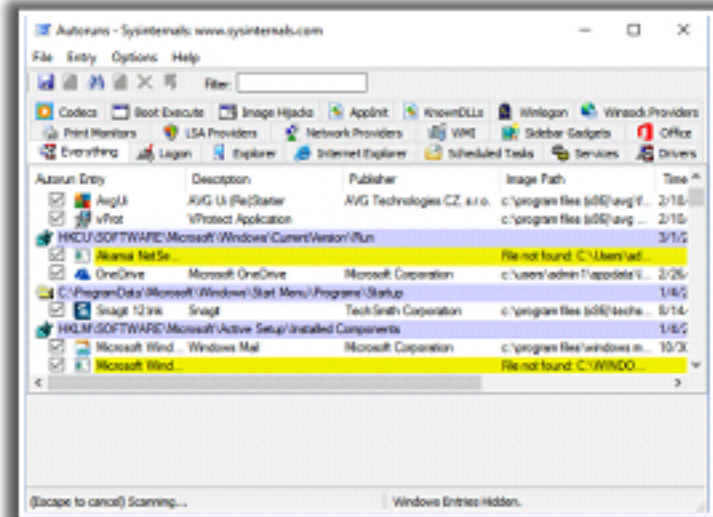


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerating Autostart Registry Locations



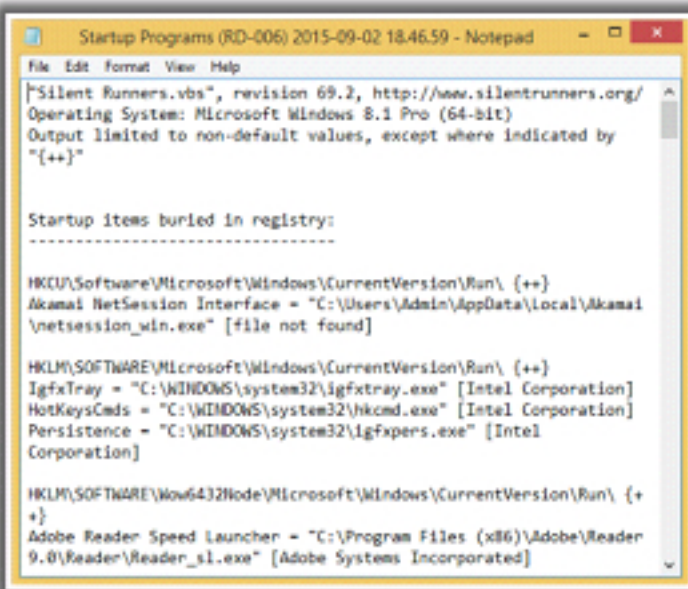
- **AutoRuns** tool can be used to retrieve information from autostart locations in the registry on a live system
- AutoRuns retrieves entries from a number of registry keys and display what it finds
- It will also retrieve the **description** and **publisher** from the executable file pointed by each registry value



<https://technet.microsoft.com>

- This information assists investigators to check if anything **suspicious** is running in the autostart locations
- Visual Basic Script called **Silent Runners** is the tool for enumerating the contents of autostart registry locations

Note: The script is not compatible with **Windows 10**



<http://www.silentrunners.org>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Auto-start locations are mainly targeted by the attackers. The attackers get hold of these locations while the user performs any network based activity, for instance opening any web based application like Microsoft Outlook or the Internet Explorer. A couple of examples of auto-start locations where the attackers can introduce malwares are listed in the slide. Attackers find these registry keys extremely useful for maintaining malwares, regularly checking them to ensure that they are running fine.

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It monitors and records all activities performed against the Microsoft Windows Registry. On running this tool, it can be noticed that there were a significant number of accesses to the Registry even when there is apparently no user intervention. This tool gives a great deal of information to the forensic investigators to trace out any intrusion on a system. The Process Monitor tool is compatible with Windows Vista and higher.

The information retrieved using the Autoruns tools provide a way to the forensic investigators to trace any suspicious activity that has taken place within the Autostart locations. Autoruns are updated regularly so that they provide the most comprehensive list of Registry keys of the autostart locations.

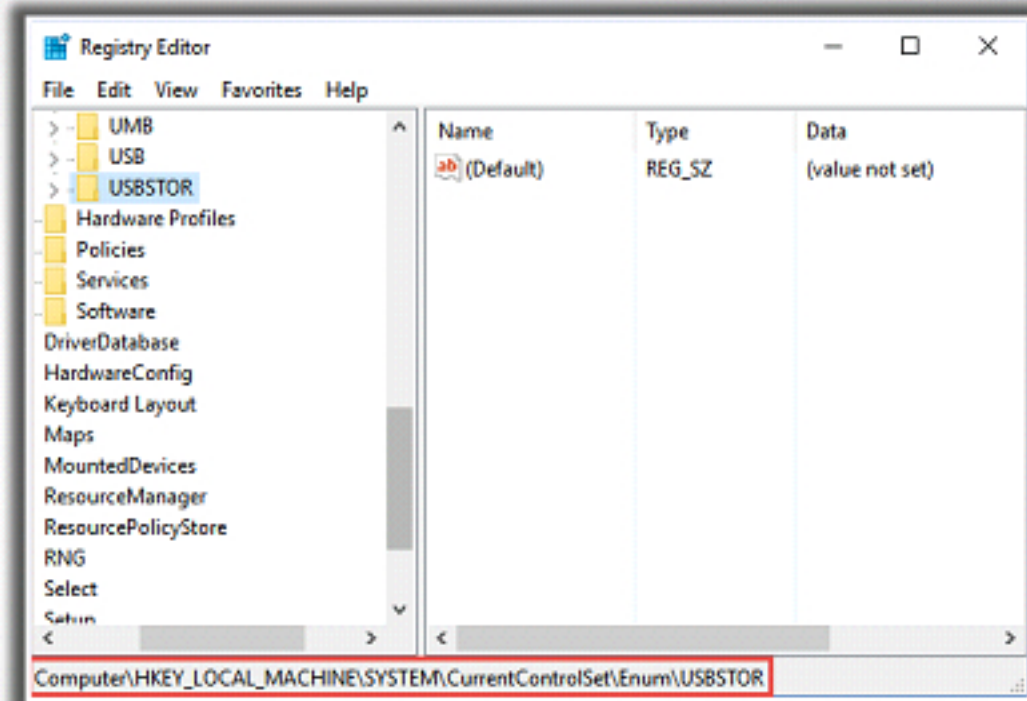
While performing an investigation, the experts require tools that can permit viewing as well as enumeration of a Registry that has been reconstructed from the component files with a system image. One such tool that serves this dual purpose is the Visual Basic script called Silent Runners. The main purpose of this tool is to enumerate the contents of the autostart Registry locations, providing the investigators further details on these suspicious activities.

USB Removable Storage Devices



- When a USB device is connected to a Windows system, **footprints** or **artifacts** are left in the registry
- When the device is plugged in, the **Plug and Play (PnP) Manager** receives the event and queries the device descriptor in the firmware for device information
- The PnP Manager then uses this information to **locate the appropriate driver** for the device and, if necessary, loads that driver
- Once the device has been identified, a **registry key** is created beneath the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

USB Removable Storage Devices (Cont'd)



- Beneath the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR** key, subkeys that are created are named with the following form: **Disk&Ven_###&Prod_###&Rev_###**
- This subkey represents the device class identifier. The fields represented by **###** are filled in by the PnP Manager based on information found in the device descriptor
- For example: The class ID for a 1GB Geek Squad thumb drive purchased from Best Buy looks like: **Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev_6.15**
- You can use **USBDeview** to view the contents of the device descriptor

- iManufacturer** and **iProduct** information from the device descriptor is mapped to the device class ID
- iSerialNumber** is a unique instance identifier for the device, similar to the MAC address of a network interface card

```
Command Prompt

iManufacturer:                0x01
    English (United States)    "Best Buy"
iProduct:                     0x02
    English (United States)    "Geek Squad U3"
iSerialNumber:                 0x03
    English (United States)    "0C90195032E36889"
```

Portion of the Device Descriptor for the Geek Squad Thumb Drive

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

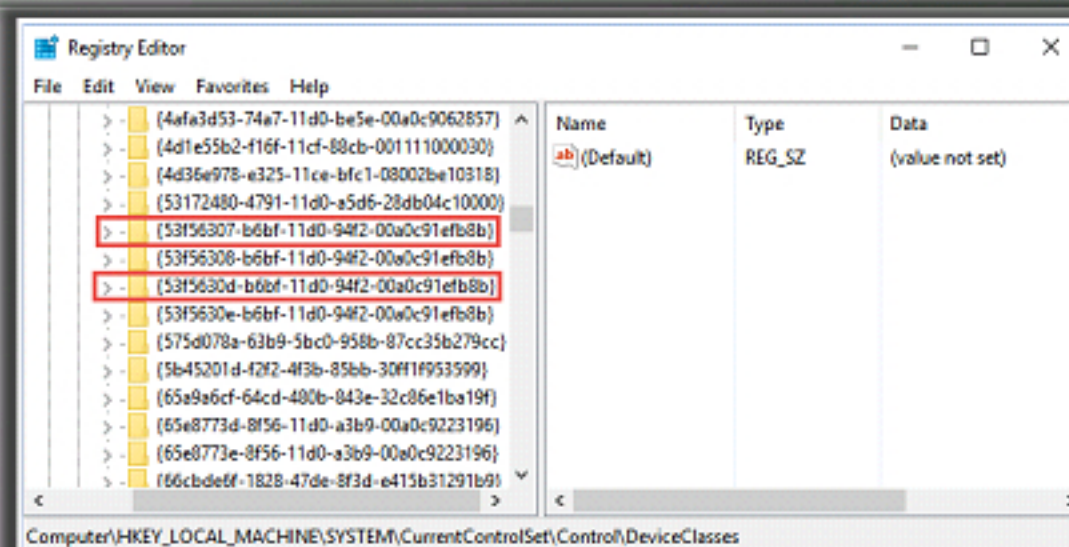
USB Removable Storage Devices (Cont'd)



- **ParentIDPrefix** value can be used to **correlate additional information** within the registry, which is important for investigation
- Using both the **unique instance identifier** and the **ParentIDPrefix**, the last time the USB device was connected to the Windows system can be determined
- Navigate to the following key to find specific device classes:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses



- Below this key there are **subkeys**, the specific device classes that are of interest include:
{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
and {53f5630db6bf-11d0-94f2-00a0c91efb8b}
- They are **GUIDs** (globally unique identifiers) for the disk and volume device interfaces



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

USB Removable Storage Devices (Cont'd)



- Navigate to {53f56307-b6bf-11d0-94f2-00a0c91efb8b} GUID and look for the **subkey**:
 - USBSTOR#Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev_6.15#**0C90195032E36889&0**{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
- The highlight represents the **unique instance identifier** within the key name
- The **LastWrite** time of this key corresponds to the **last time the disk device** was connected to the system



- Similarly, conduct the same correlation with the volume device interface GUID, using the **ParentIDPrefix** for the device, as below:
 - **##?#STORAGE#RemovableMedia#7&326659cd&0&RM#**{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
- The highlight represents the **ParentIDPrefix** within the device subkey
- The **LastWrite** time of this key corresponds to the **last time the volume** was connected to the system.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The USB removable devices connected across a Windows system can be tracked using the footprints or artifacts left by them in the registry. The Artifacts are also left in the setupapi.log file.

Plug and Play (PnP) Manager

Plug and Play (PnP) is a combination of hardware technology and software techniques that enables a PC to recognize when a device is added to the system. With PnP, the system configuration can change with little or no input from the user. For example, when a USB thumb drive is plugged in, Windows can detect the thumb drive and add it to the file system automatically. However, to do this, the hardware must follow certain requirements and so also the driver.

USBDeview

USBDeview is a small utility that lists all USB devices that are currently connected to a computer, as well as all the previously connected USB devices. For each USB device, extended information is displayed i.e., the Device name/description, device type, serial number (for mass storage devices), the date/time that device was added, VendorID, ProductID, and more. USBDeview also allows the user to uninstall USB devices that have been used previously, disconnect USB devices that are currently connected to the computer, as well as disable and enable USB devices. USBDeview can also be used on a remote computer, as long as the user is logged in to that computer as an admin user.

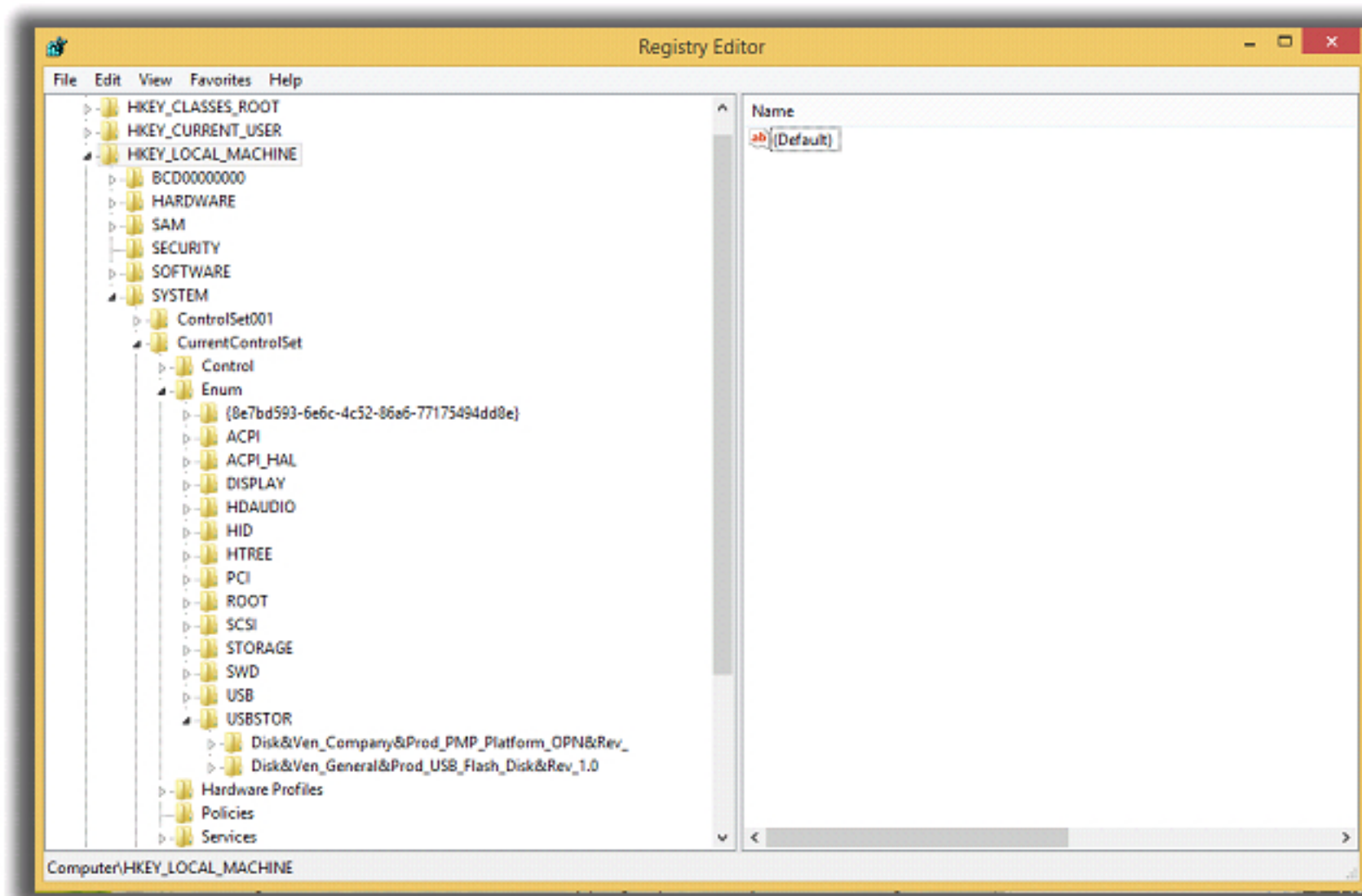


FIGURE 6.2: USBOR key in Registry Editor

The figure represents a portion of RegEdit showing Device Class ID and Unique Instance ID.

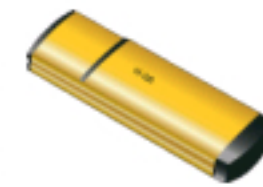
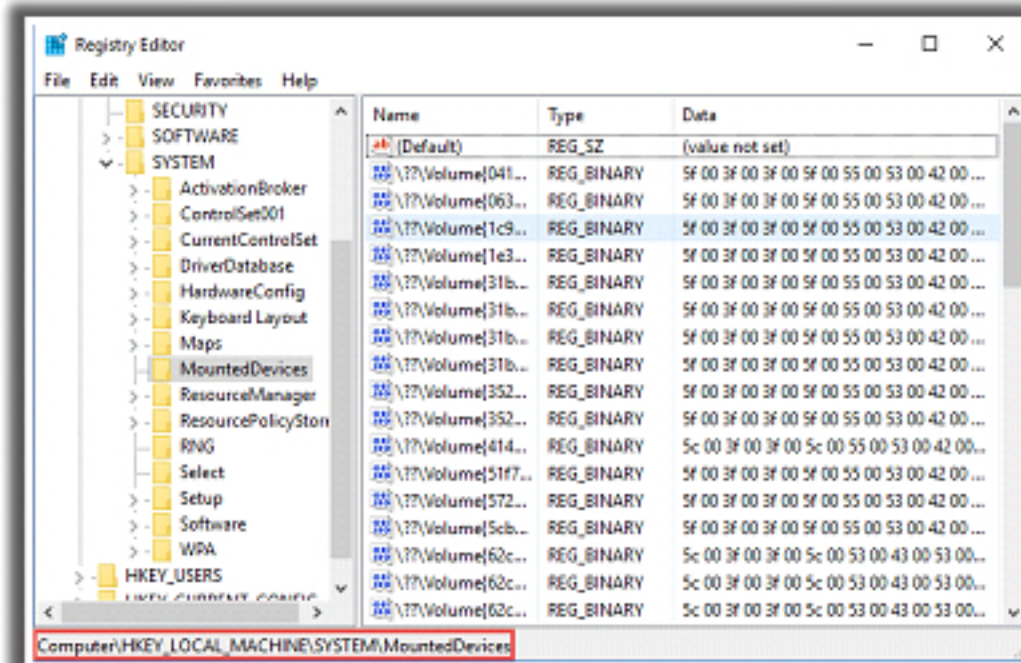
Mounted Devices



The **MountedDevices** key stores information about the various devices and volumes mounted on an NTFS file system

The complete path to the key:
HKEY_LOCAL_MACHINE\System\MountedDevice

When a USB removable storage device is connected to a Windows system, it is assigned a drive letter; that shows up in the **MountedDevices** key. For e.g. If the device is assigned the drive letter F:, the value in the **MountedDevices** key will appear as **\DosDevices\F:**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mounted Devices (Cont'd)



ParentIdPrefix value found within the unique instance ID key can be used to map the entry from **USBSTOR** key to the **MountedDevices** key

This can be done by right-clicking each of the **Registry** values and choosing **Modify...**

When the **Edit Binary Value** dialog opens, check for the presence of **ParentIdPrefix** value

The **ParentIdPrefix** value is stored in the Registry as a string, but the **DosDevices** values within the **MountedDevices** Registry key are stored as binary data types, so translation is required

Drive letter assigned to the device can be located using the **ParentIdPrefix** value to map between the **USBSTOR** and **MountedDevices** registry keys

Find references in other locations in the Registry or in Shortcut files that point to the drive and then correlate the **LastWrite** times of the **unique instance ID key**, the **MountedDevices** key, and the **MAC times** on files to develop a timeline

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

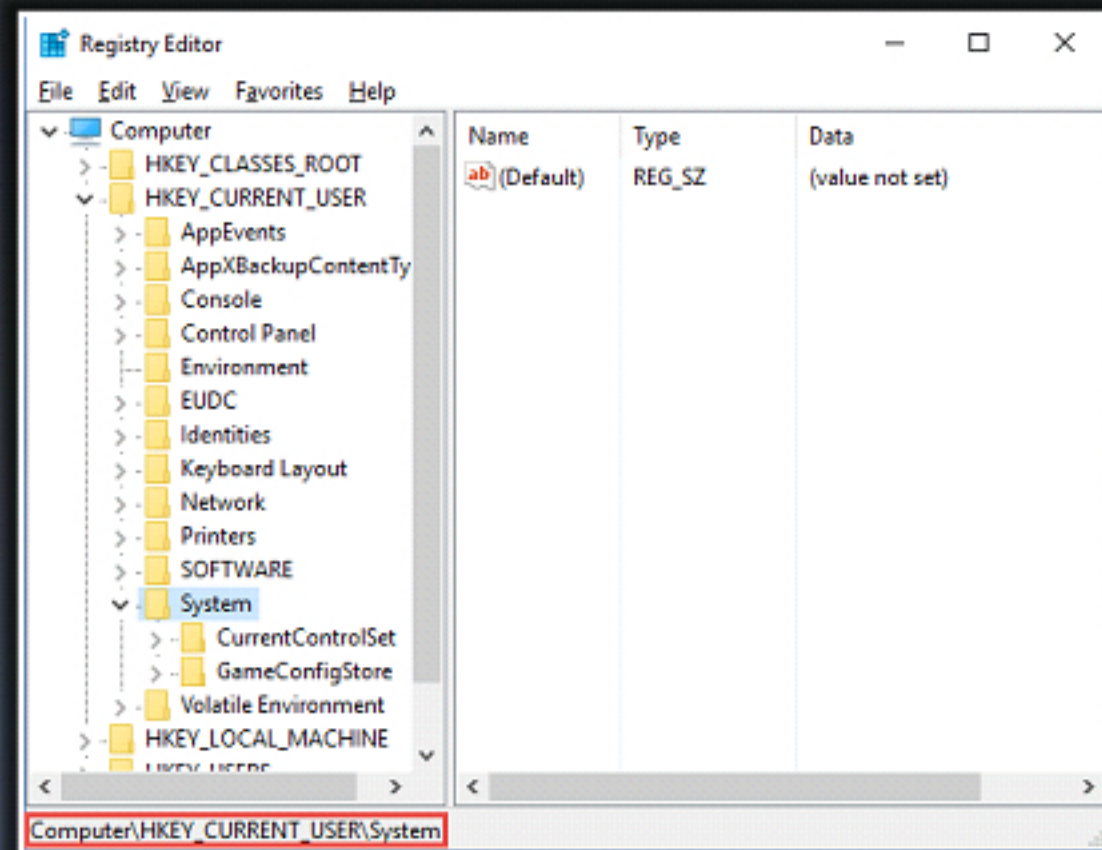
Any external device attached to a system will leave artifacts in several locations. Forensic investigators review these artifacts and concentrate on the ones which are of forensic importance. This depends upon the type of investigation that is being conducted. In a Windows system, the Registry keys track every device that is connected to the computer and the allotted drive letter used by the NTFS file system.

Few of the registry keys record the information related to external devices that has been connected to the system in the past. Examples of few external devices include portable hard disks, magnetic tape, memory stick / flash drive, solid state memory cards, DVD or CDs. These keys can be retrieved from a live system by running "regedit" or "Registry Commander" via an externally connected USB drive and can be saved as readable text files.

Tracking User Activity

CHFI
Computer Hacking Forensic Investigator

- Registry keys that track user's activities can be found in the **NTUSER.DAT** file
- When a user performs a particular action, the registry key's **LastWrite** time is updated
- Also, there are keys that track user activities and **add or modify timestamp information** associated with the registry values, this timestamp information is maintained in the value data
- The majority of the user's activities is recorded in the **HKEY_CURRENT_USER** hive



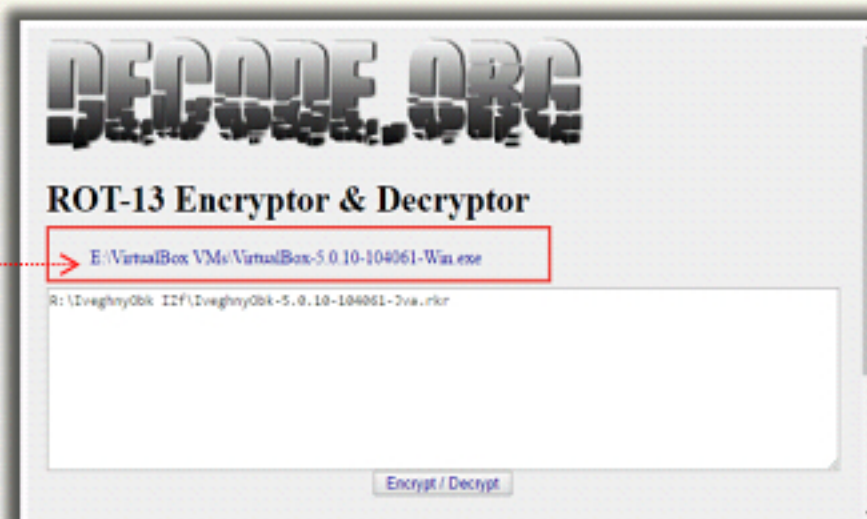
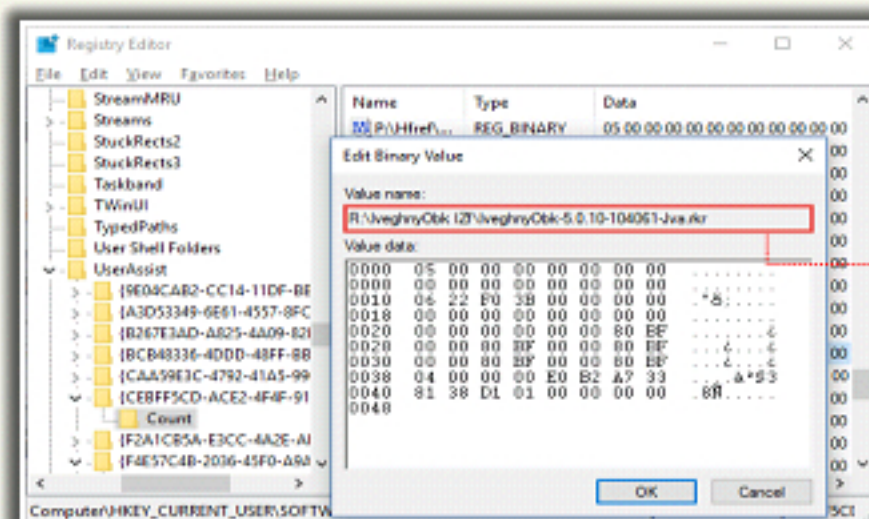
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The UserAssist Keys

CHFI
Computer Hacking Forensic Investigator

- You can find user information stored in the user's NTUSER.DAT file beneath the following registry key:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count
- Below the UserAssist key, there are GUIDs such as:
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA} and
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
- Each GUID records values pertaining to specific objects the user has accessed on the system such as shortcut files, control panel applets, programs, etc.

- The values are encoded with ROT-13 encryption algorithm (Caesar cipher) in which each letter is replaced with the letter 13 letters after it in the alphabet
- Use **ROT-13 Encryptor & Decryptor** to decrypt the value names
- UserAssist key gives information on what types of files or applications have been accessed on a particular system



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

MRU Lists

**1**

Applications maintain an Most Recently Used (MRU) list, which is a **list of files** that have been most **recently used**

2

Within the running application, these file names generally appear at the bottom of the drop-down menu when **File** on the menu bar is selected

3

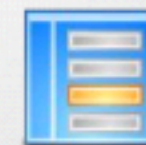
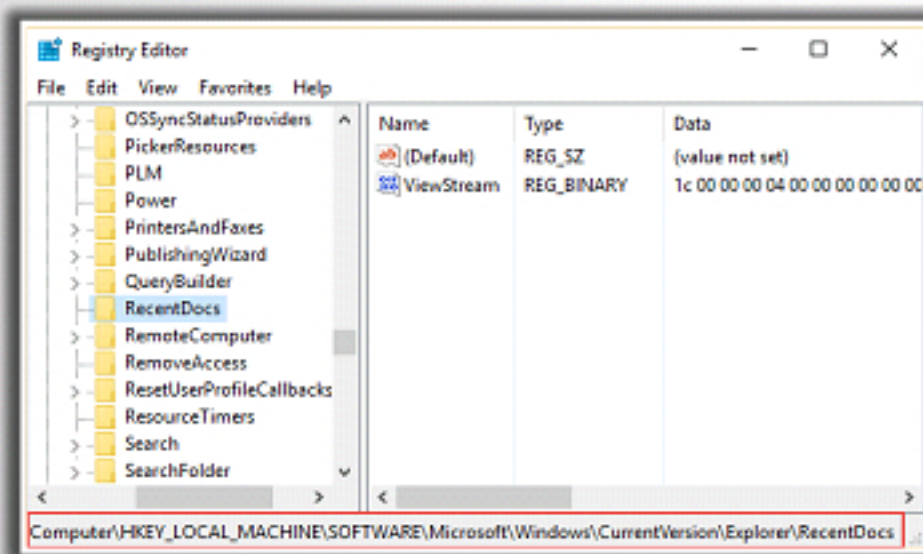
Find the MRU list registry key at:

• `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`

4

MRU list has two sections:

- The numbered value names: It contains the **names** of the files accessed
- **MRUListEx** key: It maintains the **order** in which the files are accessed



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

MRU Lists (Cont'd)

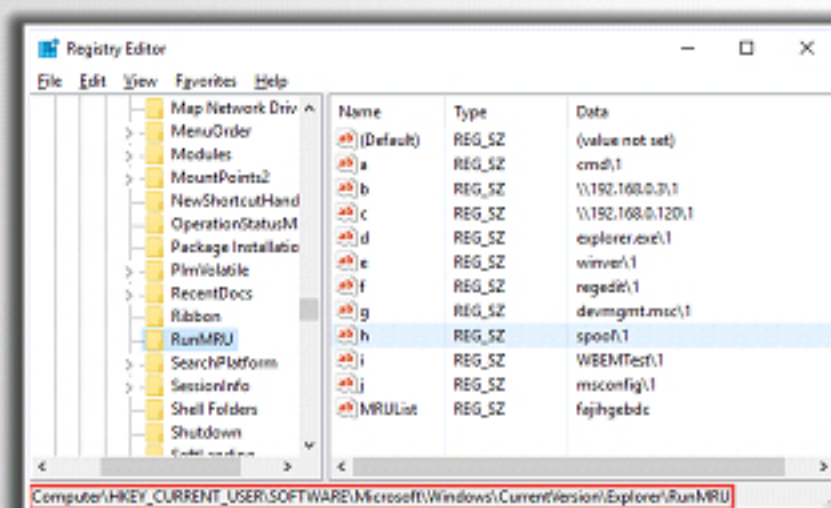


RunMRU

Another MRUList can be found in the RunMRU key:

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

Entries are added to this key when a user clicks the **Start** button, chooses **Run**, and types a command or the name of a file

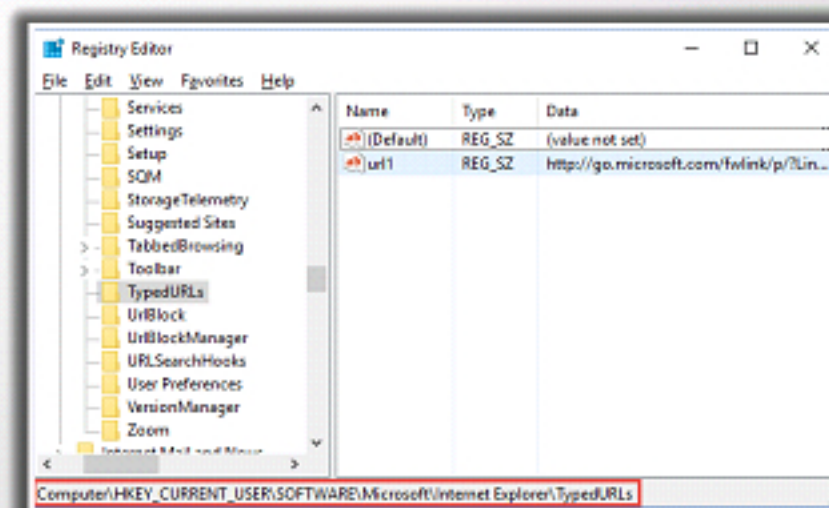


TypedURL

Another key similar to the RunMRU key is the TypedURLs key:


`HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs`

This key maintains a MRU list of URLs that a user types into the address bar



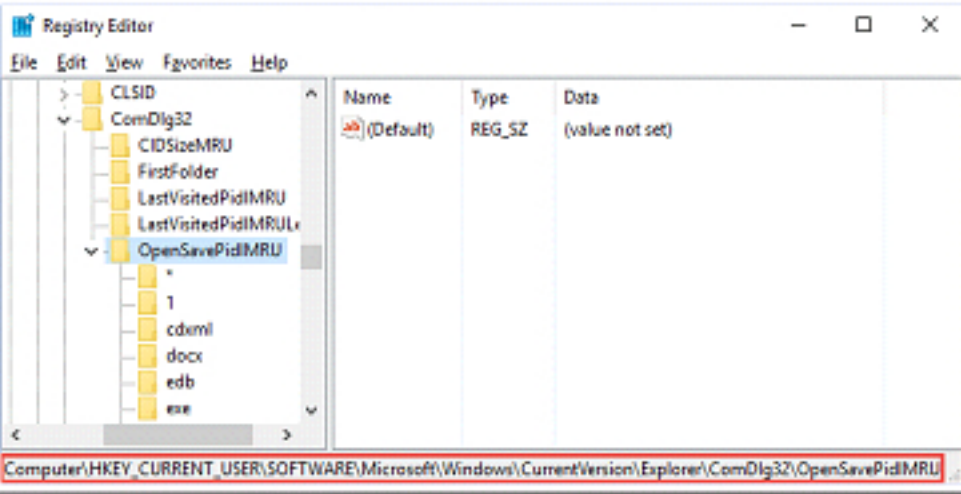
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

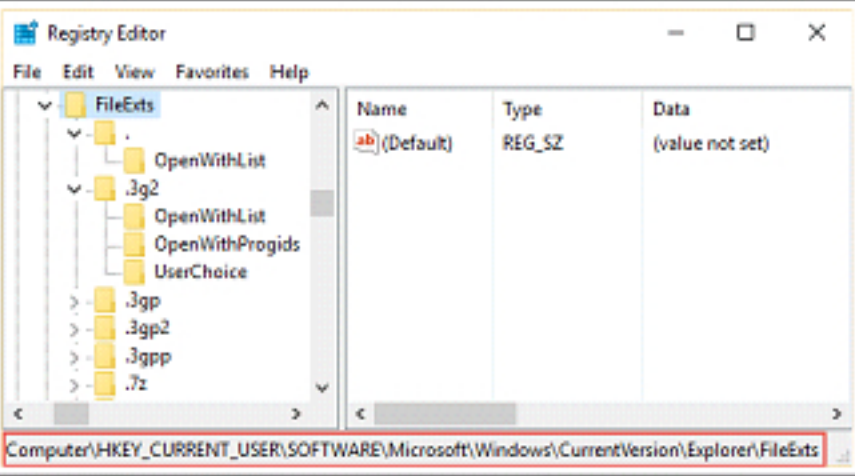
MRU Lists (Cont'd)



Another key that holds MRU lists is the following:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU

This key maintains MRU lists of files opened via **Open** and **SaveAs** dialogs within the Windows shell





Another key that holds MRU lists is the following:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts

The subkeys beneath this key correspond to extensions for files that have been opened on the system. Below the file extension subkeys, subkeys called **OpenWithProgids** and **OpenWithList** are present. These registry entries tell the system what application to use to open a file with that extension when the file is double clicked

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Most Recently Used lists, abbreviated as MRU list are the lists of recently visited web pages, opened documents, etc., maintained by the Windows operating system in the Windows Registry. Many applications also maintain an MRU list. Within the running application, these file names generally appear at the bottom of the drop-down menu when a file on the menu bar is selected.

The MRU list registry key is the RecentDocs key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

This key can contain a number of values, all of which are binary data types. The values investigators are interested in are the ones that have names, especially the one named MRUListEx.

The numbered value names contain the names of the files accessed (in Unicode), and the MRUListEx key maintains the order in which they were accessed (as DWORDs).

The RecentDocs key also has a number of sub-keys. Each one of these sub-keys are actually the extension of a file that was opened (.doc, .txt, .html, etc.). The values within these sub-keys are maintained in the same way as in the RecentDocs key: the value names are numbered, and their data contains the name of the file accessed as a binary data type.

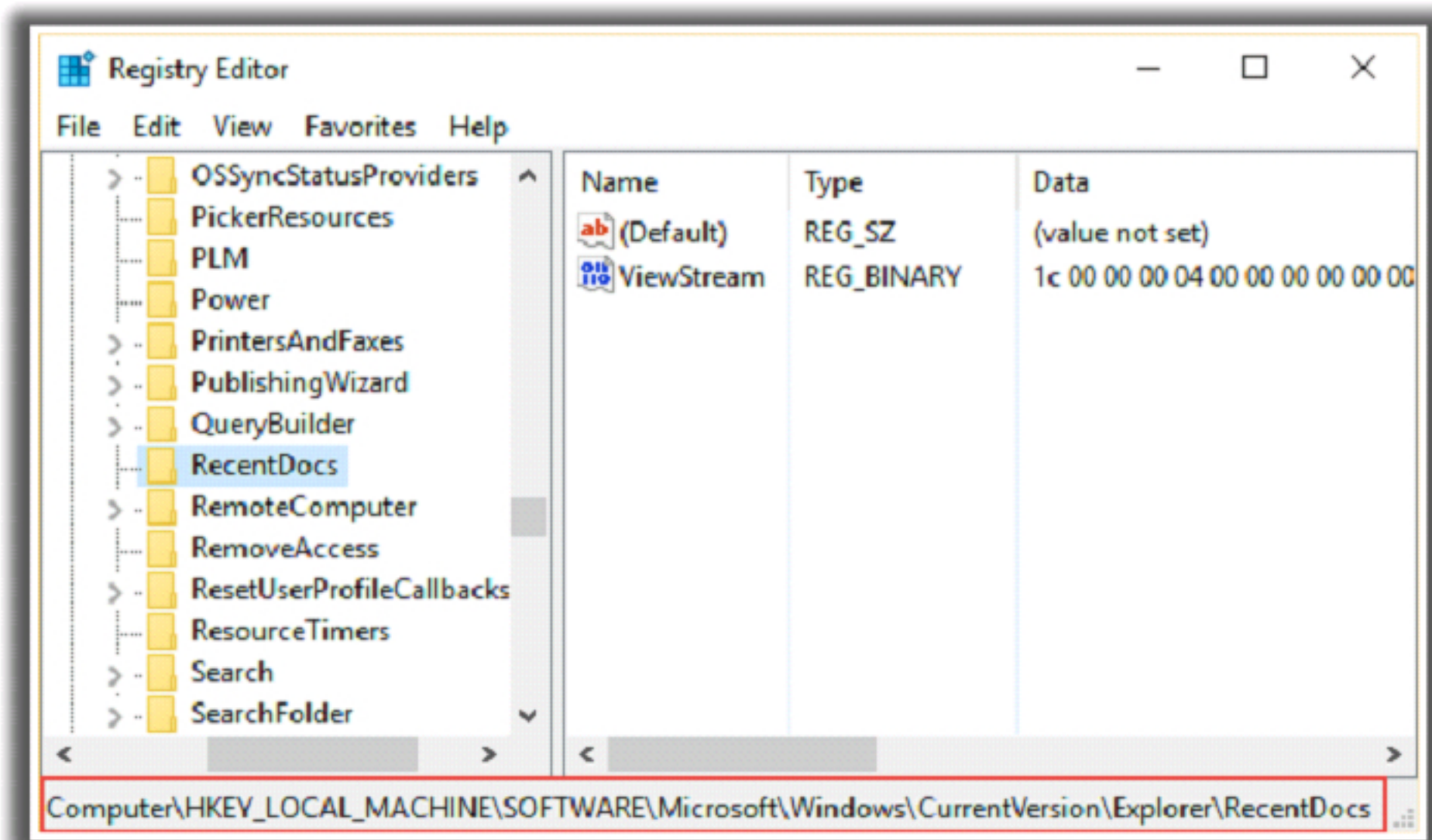


FIGURE 6.3: RecentDocs key in the Registry Editor

Connecting to Other Systems



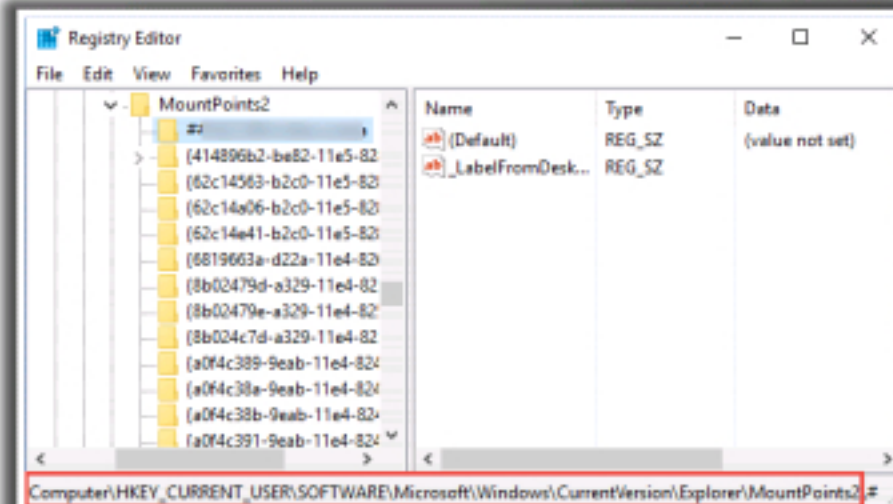
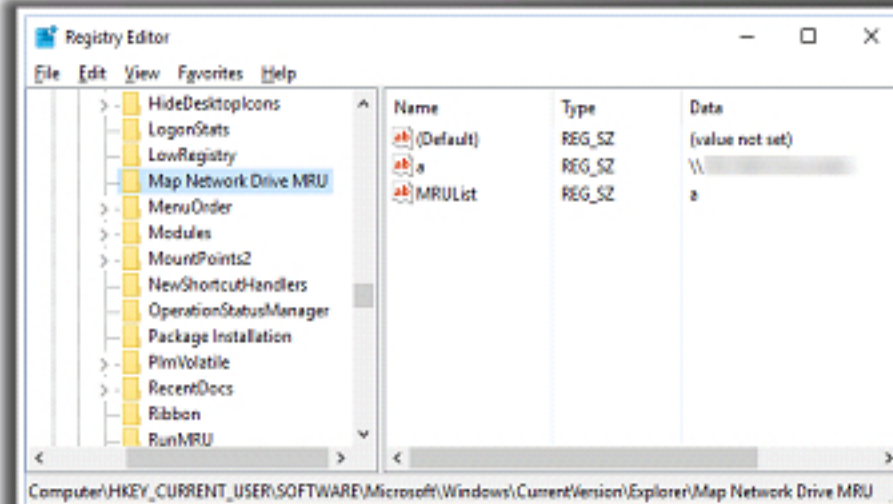
- When a user uses the Map Network Drive Wizard to connect to a remote system, an MRU list is created beneath the following key:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU

- Each entry is given a letter as the value name, and the MRUList value represents the order in which the user connected to each drive or share

- Whether the user uses the **Map Network Drive Wizard** or the **net use** command, the volumes the user added to the system will appear in the following key:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Restore Point Registry Settings



- The purpose of restore points is to take a snapshot of the system so that a user can restore the system to a previous restore point, if things went wrong

- The settings for restore points are stored in the registry at:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRestore

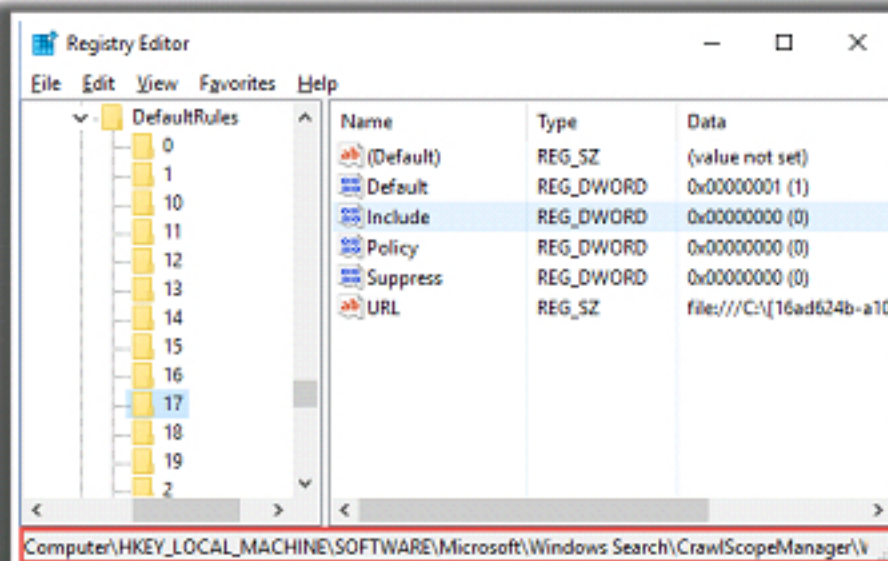
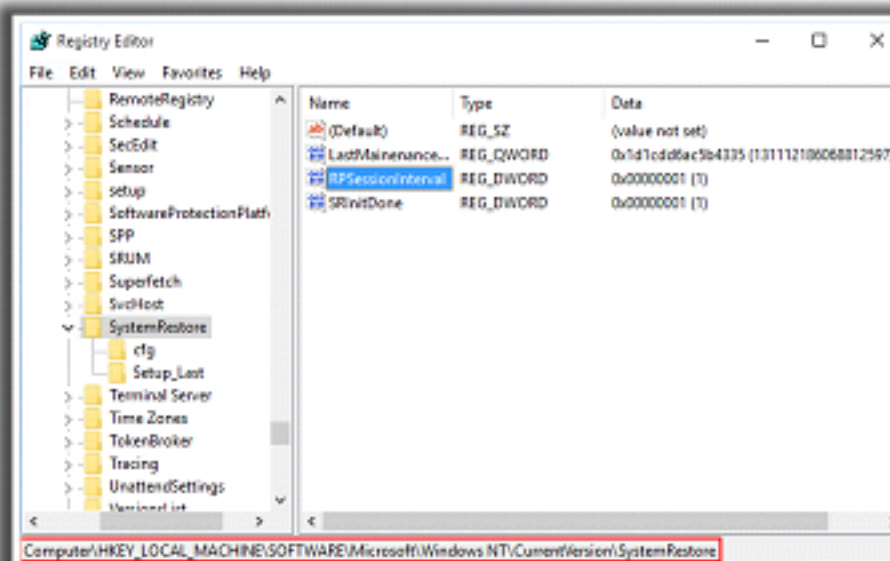
- The interval for restore point creation is stored in the **RPSessionInterval** value

- Find restore points in numbered folders in the following location:

\System Volume Information\ - restore {GUID}\RP##


- Path to navigate to **System Restore**:

Right-click **Start** → **Control Panel** → **System and Security** → **System** → **System protection link** → **System Restore...**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

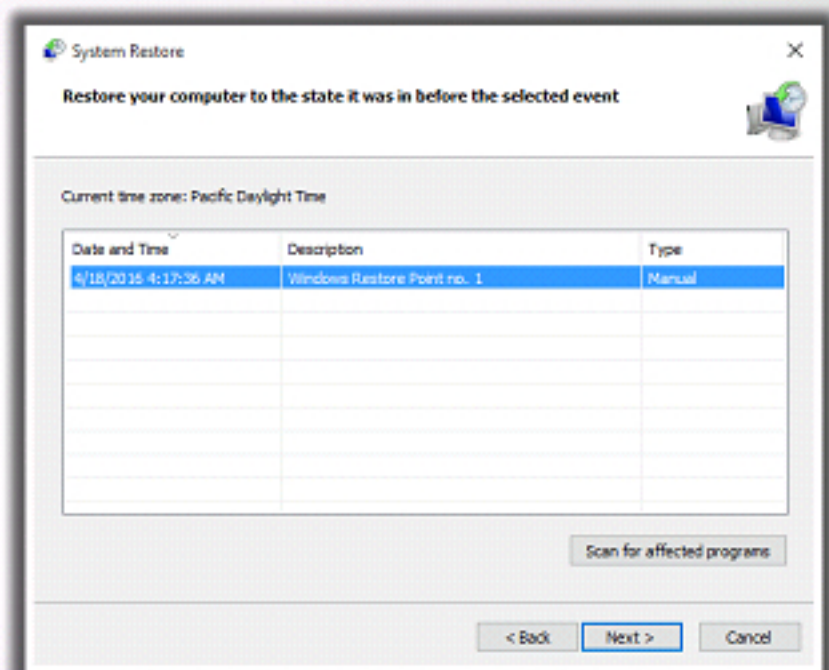
Analyzing Restore Point Registry Settings (Cont'd)




Automatically created restore points have names assigned to them that are stored in the file `rp.log` located in the root of the folder `RP##`

Characteristics of restore point and their names:

- ❌ When restore points are created on schedule, they are named **System CheckPoints**, which appears in the user interface
- ❌ The restore point name is stored starting at byte offset 16 in the `rp.log` file
- ❌ If software or **unsigned drivers** are installed, the system usually creates a restore point. The name of the software or the unsigned driver is used as the name of the restore point
- ❌ A user can manually **create restore points**, and the user-provided name is stored in this same location
- ❌ The last 8 bytes of the `rp.log` file are a **Windows 64-bit time stamp** indicating when the restore point was created



Date and Time	Description	Type
4/18/2016 4:17:36 AM	Windows Restore Point no. 1	Manual



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The purpose of restore points in general is to take a snapshot of a system, so that the user can restore the system to a previous restore point if something goes wrong.

The settings for restore points are stored in the registry. They are stored at:

`HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore`

The information about the interval for restore point creation is stored in the `RPGlobalInterval` value, and the default `DWORD` data is 86,400. The system restore points can be reset and disabled. The setting for disabling restore points is a value named `DisableSR` and it defaults to 0. If the setting has been changed to 1, it means that the restore point creation has been disabled.

The investigator can find restore points in numbered folders at:

`\System Volume Information\restore {GUID}\RP##`

Neither user nor administrator can access files and folders below the system volume information by using the Explorer interface, therefore the users find it difficult to access, manipulate, or delete these files.

The navigation to System Restore is as follows:

Select **Start → All Programs → Accessories → System Tools → System Restore** to open the UI for System Restore.

Determining the Startup Locations



Common startup locations in the registry are listed below:

Registry Key	Notes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\	All values in this key are executed at system startup
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\	All values in this key are executed at system startup and are deleted later
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	The value Shell will be executed when any user logs on. This value is normally set to explorer.exe, but it could be changed to a different Explorer in a different path

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determining the Startup Locations (Cont'd)



Registry Key	Notes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\	Each subkey (GUID name) represents an installed component. All subkeys are monitored, and the StubPath value in subkeys, when present, is a way of running code
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\	Value Load, if present, runs using explorer.exe after it starts
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager	The value BootExecute contains files that are native applications executed before Windows Run
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\	This contains a list of services that run at system startup. If the value Start is 2, startup is automatic. If the value Start is 3, startup is manual and starts on demand for service. If the value Start is 4, service is disabled
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\	The subkeys are for layered service providers, and the values are executed before any user logs in

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determining the Startup Locations (Cont'd)



Registry Key	Notes
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\	All values in this subkey run when this specific user logs on, as this setting is user specific
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\	All values in this subkey run when this specific user logs on, and then the values are deleted
HKEY_CURRENT_USER\Control Panel\Desktop	For this specific user, if a screensaver is enabled, a value named scrnsave.exe is present. Whatever is in the path found in the string data for this value will execute when the screensaver runs
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\	For this specific user, the string specified in the value run executes when this user logs on

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determining the Startup Locations (Cont'd)

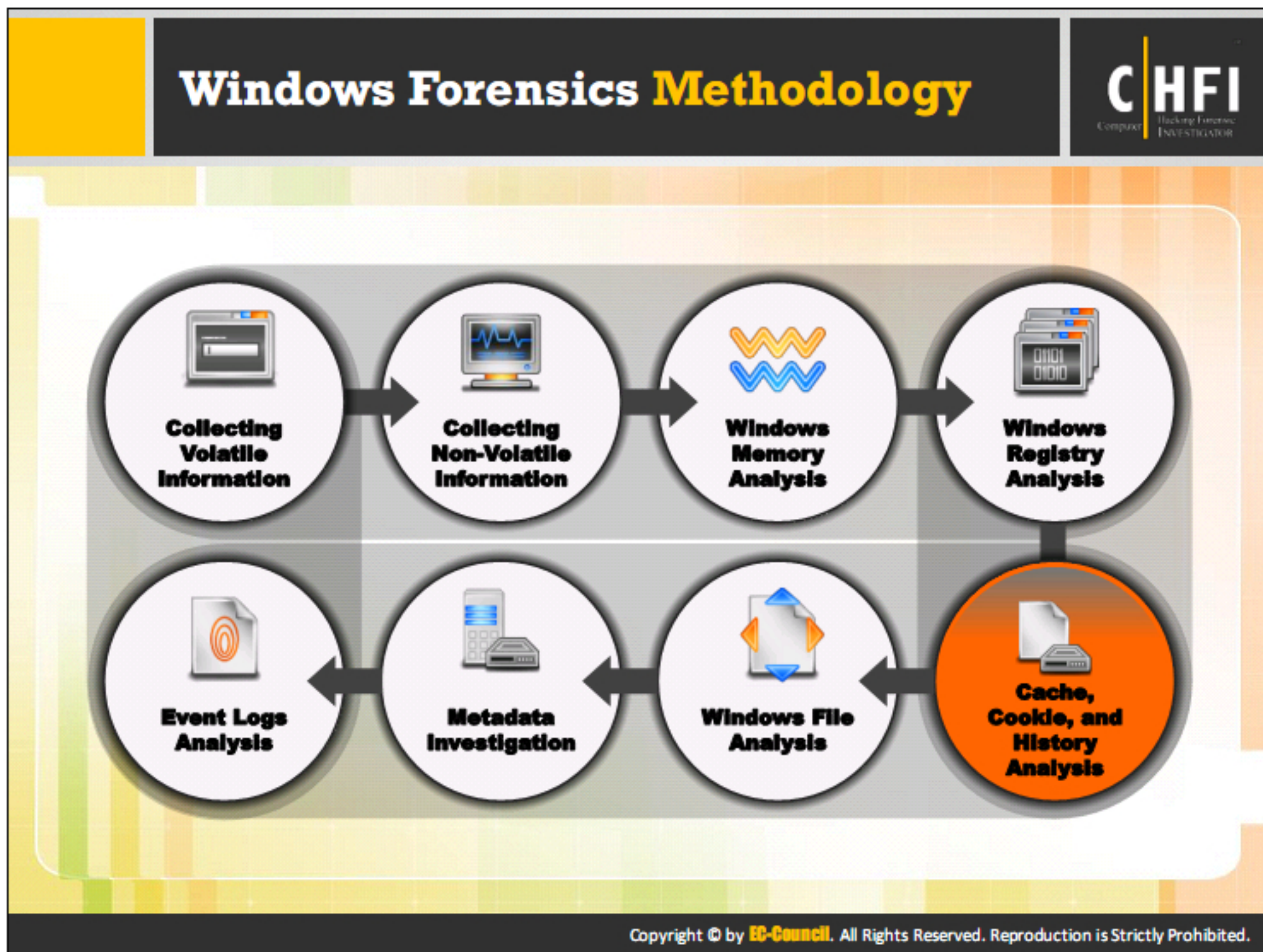


User Startup Folder Registry Settings are as shown below:

Registry Key	Default or Normal Settings
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Value Startup will be C:\Documents and Settings\%UserName%\Start Menu\Programs\Startup where %UserName% will not be the environment variable but will actually specify the user's name
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Value Startup will be %USERPROFILE%\Start Menu\Programs\Startup
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Value Common Startup will be C:\Documents and Settings\ All Users\Start Menu\Programs\Startup
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Value Common Startup will be %ALLUSERSPROFILE%\Start Menu\Programs\Startup

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Startup locations are folders and registry items where the programs run automatically, without user intervention. Many applications (for instance firewalls, anti-viruses) run automatically when the user starts his/her computer and loads the operating system. However, in some cases there are programs that are not legitimate, like Trojans, worms, spyware, viruses, etc., and can be run automatically. The attackers use the autostart locations to automatically run these malwares, and when the system boots itself these malwares corrupt the system. Therefore, it is essential to regularly check the startup registry keys in the System Configuration utility and delete the unwanted keys. Users can view the Startup list present in the System Configuration utility by choosing **Run**, typing **msconfig** into the text box, and then pressing **Enter**.



Operating systems use applications called browsers to connect with internet and allow users to access the external servers and cloud data. The browsers save data on the system in the form of cache, cookies, and history. Investigators can gather this information and analyze it to find the type of connections the system had made, protocols it used, websites visited, content accessed and downloaded.

Cache, Cookie, and History Analysis: Mozilla Firefox



Mozilla Firefox - Cache, Cookies, and History are stored in the following system locations:

Cache Location:

C:\Users\<Username>\AppData\Local\Mozilla\Firefox\Profiles\XXXXXXXX.default\cache2

Cookies Location:

C:\Users\<Username>\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\cookies.sqlite

History Location:

C:\Users\<Username>\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\places.sqlite

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analysis Tool: MZCacheView



- MZCacheView reads the cache folder of **Firefox/Mozilla/Netscape** Web browsers, and displays the list of all files currently stored in the cache
- It displays information such as **URL, Content type, File size, Last modified time, Last fetched time, Expiration time, Fetch count, Server name**, etc. for each cache file

Filename	Content Type	URL	File Size	Fetch Count	Last Modified
gmail.min.js	text/javascript	https://www.google.com/intl/en/...	38,330	1460980205	4/18/2016 4:
google.js	text/javascript	https://www.google.com/js/google...	1,935	1460980205	4/18/2016 4:
googleleg_lodpico	image/x-icon	https://www.google.co.in/images/...	1,517	1197211648	4/18/2016 4:
googlelogo_color_116...	image/png	https://www.google.com/images/b...	2,408	1460980205	4/18/2016 4:
googlelogo_color_272...	image/png	https://www.google.co.in/images/...	5,969	1460980136	4/18/2016 4:
googlemail-16.png	image/png	https://www.google.com/images/i...	739	1460980206	4/18/2016 4:
il_1967ca6a.png	image/png	https://ssl.gstatic.com/gb/images/i...	8,056	1460980136	4/18/2016 4:
ic_wahlberg_product...	image/png	https://www.google.co.in/images/...	2,091	1460980136	4/18/2016 4:
id=GTM-MW3R5V8&l...	application/javascript...	https://www.googletagmanager.co...	51,358	3819896832	4/18/2016 4:
init	application/javascript...	https://apis.google.com/js/rpcshin...	5,044	1460980206	4/18/2016 4:
k3k702ZOKLJc3Wju...	font/woff2	https://fonts.gstatic.com/s/opensa...	16,276	1460980207	4/18/2016 4:
lightbox.css	text/css	https://www.google.com/css/gweb...	1,395	1460980205	4/18/2016 4:
linkid.js	text/javascript	https://www.google-analytics.com...	852	2537947136	4/18/2016 4:
maia.css	text/css	https://www.google.com/css/maia...	12,081	1460980205	4/18/2016 4:
maia.experimental.css...	text/css	https://www.google.com/css/maia...	12,012	1460980205	4/18/2016 4:
maia.js	text/javascript	https://www.google.com/js/maia...	2,767	1460980205	4/18/2016 4:
N5LbelfynPA1KT88Fv...	font/woff2	https://fonts.gstatic.com/s/roboto/...	63,156	1460980206	4/18/2016 4:
nav_logo242.png	image/png	https://www.google.co.in/images/...	21,909	1460980136	4/18/2016 4:
ocsp	application/ocsp-resp...	https://clients1.google.com/ocsp	463	1460980205	4/18/2016 4:

<http://www.nirsoft.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analysis Tool: MZCookiesView



MZCookiesView displays the **details of all cookies** stored inside the cookies file (cookies.txt) in one table, and allows to save the cookies list into a text, HTML or XML file, delete unwanted cookies, and backup/restore the cookies file

MZCookiesView: C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\5orf6e1.default\cookies.sqlite

Domain/Host	Path	Name	Value	Expiration Date
246059135.log.optimizel...	/	end_user_id	oeu1460980110627r0...	4/16/2026 4:48:33 AM
doubleclick.net	/	test_cookie	CheckForPermission	4/18/2016 5:05:09 AM
google.co.in	/	NID	78=hjQIngeemXt_gd...	10/18/2016 4:48:54 AM
google.co.in	/	OGPC	5061821-1:	6/17/2016 4:48:57 AM
google.co.in	/	OGP	-5061821:	6/17/2016 4:48:59 AM
google.com	/	NID	78=thGnN03WNYO7...	10/18/2016 4:49:00 AM
google.com	/	NID	78=dxT1n8cUTjKLQ...	10/18/2016 4:51:15 AM
mozilla.org	/	optimizelyEndUserId	oeu1460980110627r0...	4/16/2026 4:48:30 AM
mozilla.org	/	optimizelySegments	{"245617832":"none",...	4/16/2026 4:48:30 AM
mozilla.org	/	optimizelyBuckets	{}	4/16/2026 4:48:31 AM
mozilla.org	/	optimizelyPendingLogEvents	[]	4/18/2016 4:48:48 AM
mozilla.org	/	_get_UA-36116321-1	1	4/18/2016 4:58:34 AM
mozilla.org	/	_ga	GA1.2.307053417.146...	4/18/2018 4:48:56 AM
www.google.com	/intl/en/mail/help/	_utma	145581362.206324595...	4/18/2018 4:50:06 AM
www.google.com	/intl/en/mail/help/	_utmc	145581362.146098020...	10/17/2016 4:50:06 PM
www.google.com	/intl/en/mail/help/	_utmt	1	4/18/2016 5:00:06 AM
www.google.com	/intl/en/mail/help/	_utmb	145581362.1.10.14609...	4/18/2016 5:20:06 AM
accounts.google.com	/	GAPS	1:1J9K0IA4Kxfgh1L_4...	4/18/2018 4:50:04 AM

18 Cookies

<http://www.nirsoft.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analysis Tool: MZHistoryView



- MZHistoryView reads the **history data file** (history.dat) of Firefox/Mozilla/Netscape Web browsers, and displays the list of all **visited Web pages** in the last days
- It displays information such as **URL**, **First visit date**, **Last visit date**, **Visit counter**, **Referrer**, **Title**, and **Host name** for each visited Web page

MZHistoryView - C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\5orf6e1.default\places.sqlite

URL	First Visit Date	Last Visit Date	Visit Count
http://www.google.co.in/?gfe_rd=cr&ei=q8kUy7BP1cfUBMs9pKgK	N / A	4/18/2016 4:48:54 AM	1
http://www.google.com/	N / A	4/18/2016 4:48:53 AM	1
https://accounts.google.com/ServiceLogin?service=mail&passive=true&...	N / A	4/18/2016 4:50:04 AM	1
https://mail.google.com/intl/en/mail/help/about.html	N / A	4/18/2016 4:50:04 AM	1
https://mail.google.com/intl/en/mail/?tab=wm	N / A	4/18/2016 4:50:04 AM	1
https://www.google.co.in/?gfe_rd=cr&ei=q8kUy7BP1cfUBMs9pKgK&gsw...	N / A	4/18/2016 4:48:54 AM	1
https://www.google.com/intl/en/mail/help/about.html	N / A	4/18/2016 4:50:05 AM	1
https://www.mozilla.org/en-US/firefox/45.0.2/first-run/	N / A	4/18/2016 4:48:26 AM	1
https://www.mozilla.org/en-US/firefox/windows-10/welcome/?utm_sour...	N / A	4/18/2016 4:48:30 AM	1

9 item(s), 1 Selected

<http://www.nirsoft.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

MozillaCacheView

MozillaCacheView is a small utility that reads the cache folder of Mozilla/Netscape web browsers, and displays the list of all files currently stored in the cache. For each cache file, the following information is displayed: URL, content type, file's size, last modified time, last fetched time, expiration time, fetch count, server name, and more. The user can easily select one or more items from the cache list, and then extract the files to another folder, or copy the URLs list to the clipboard.

MozillaCookiesView


MozillaCookiesView is an alternative to the standard "Cookie Manager" provided by Netscape and Mozilla browsers. It displays the details of all cookies stored inside the cookies file (cookies.txt) in one table. It also allows you to save the cookies list into a text, HTML, or XML file; delete unwanted cookies; and backup and restore the original cookies file.

MozillaHistoryView

MozillaHistoryView is a small utility that reads the history data file (history.dat) of Mozilla/Netscape web browsers, and displays the list of all visited web pages in the last few days. For each visited web page, the following information is displayed: URL, first visit date, last visit date, visit counter, referrer, title, and host name.

Source: <http://www.nirsoft.net>

Cache, Cookie, and History Analysis: Google Chrome



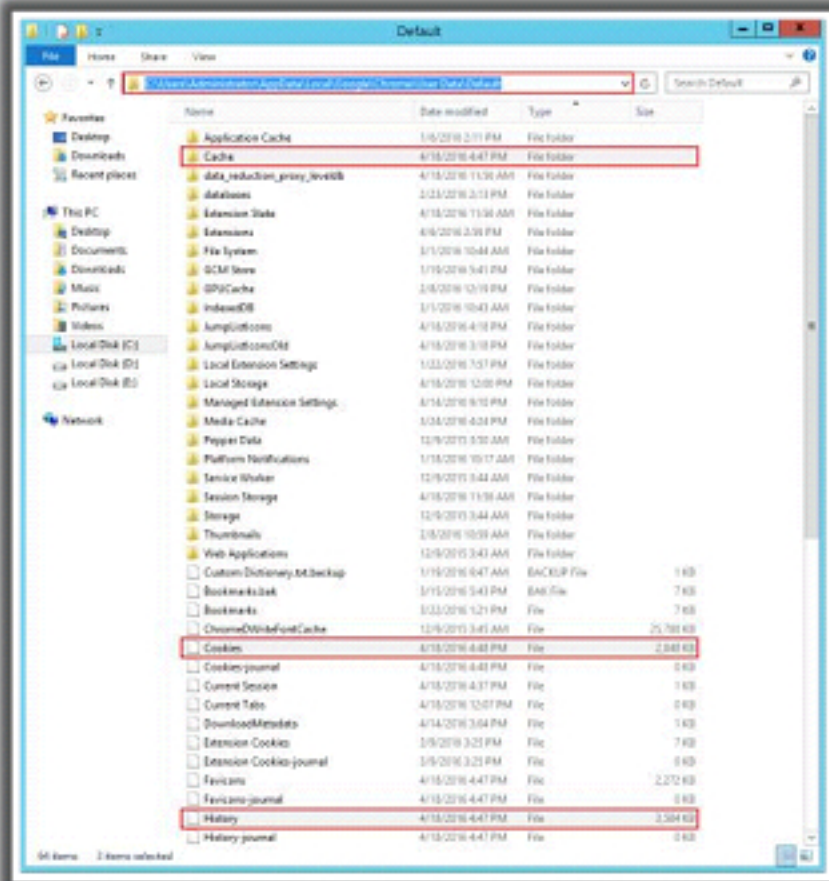
Google Chrome - Cache, Cookies, and History are stored in the following system locations:

History and Cookies Location:

C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default

Cache Location:

C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\Cache



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Google Chrome records information about browsing history on the system itself. This includes:

- History, Downloads and Cookies Location:
C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default
- Cache Location:
C:\Users\{user}\AppData\Local\Google\Chrome\User Data\Default\Cache

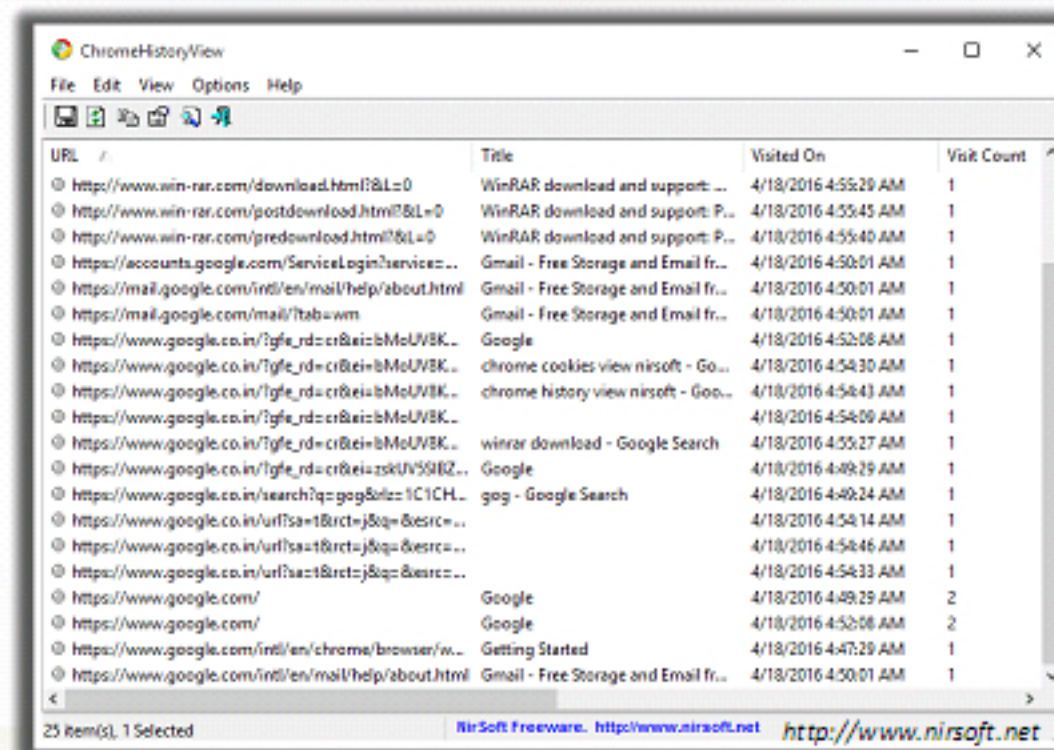


Analysis Tool: ChromeHistoryView



01 ChromeHistoryView reads the **history data file** of Google Chrome Web browser, and displays the list of all visited Web pages in the last days

02 It displays the information such as **URL, Title, Visit Date/Time, Number of visits, number of times that the user typed this address (Typed Count), Referrer, and Visit ID** for each visited Web page



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cache, Cookie, and History Analysis: Microsoft Edge



Microsoft Edge - Cache, Cookies, and History are stored in the following system locations:



Cache Location:

C:\Users\Admin\AppData\Local\Microsoft\Windows\WebCache



Cookies Location:

C:\Users\Admin\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\Cookies



History Location:

C:\Users\Admin\AppData\Local\Microsoft\Windows\History

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analysis Tool: IECacheView

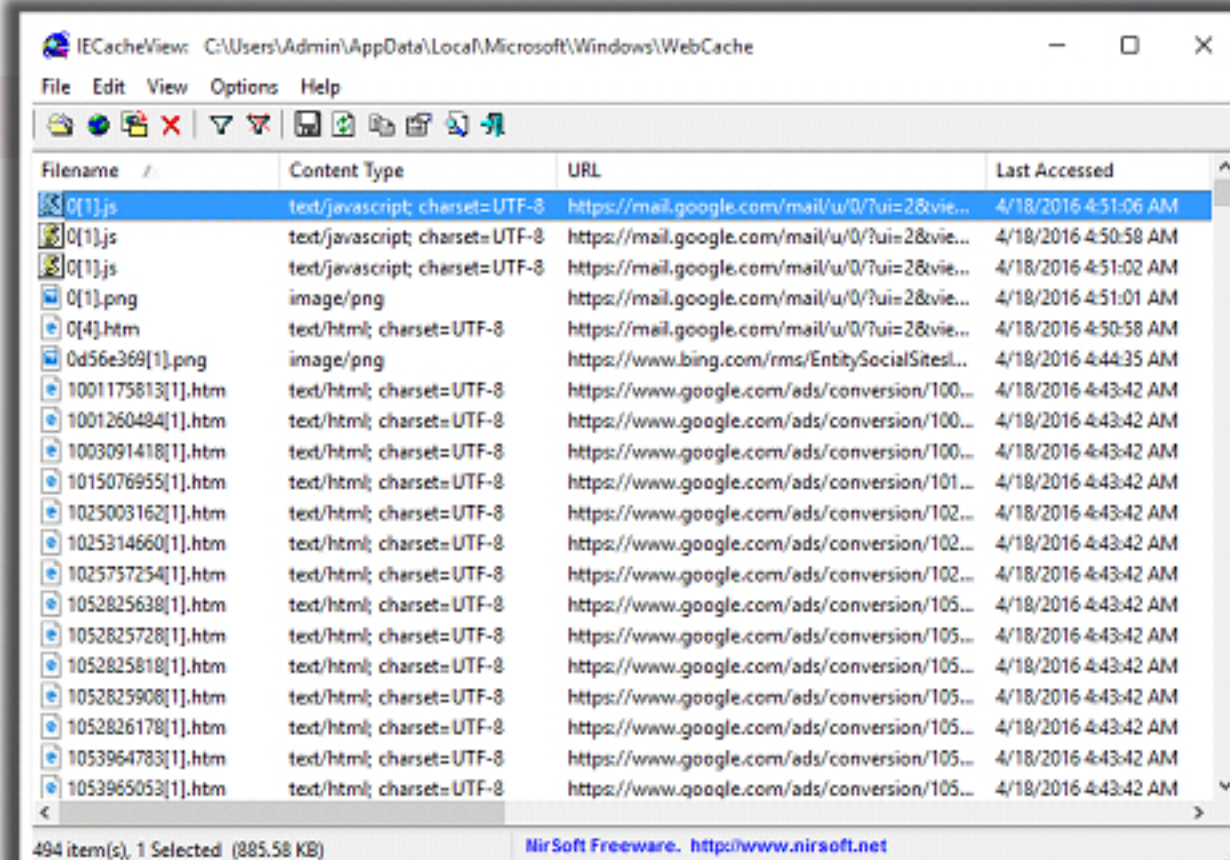
CHFI
Computer Hacking Forensic Investigator

IECacheView

It reads the cache folder of Internet Explorer, and displays the list of all files currently stored in the cache

Features

- IECacheView displays the **list of cache files**
- It allows to **filter the cache files** by file type
- It allows to **view the cache files** of another user or from another disk
- Selecting and copying the desired cache item** in the clipboard is easy

<http://www.nirsoft.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analysis Tool: IECookiesView

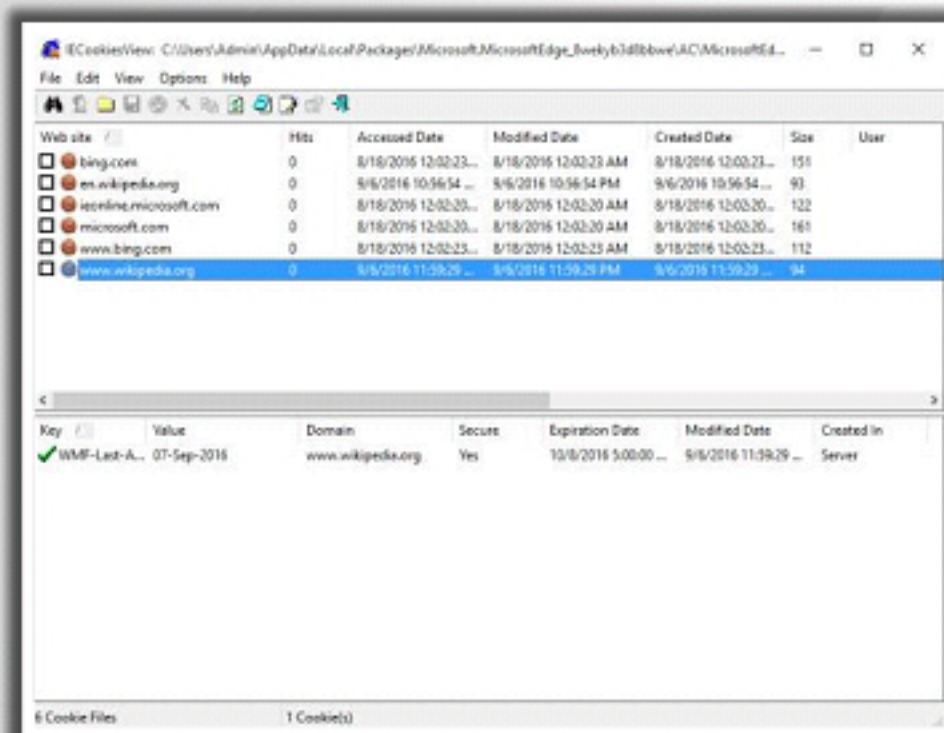
CHFI
Computer Hacking Forensic Investigator

IECookiesView

It reads the cache folder of Internet Explorer, and displays the list of all files currently stored in the cache

It allows to:

- Select and delete the **unwanted cookies**
- Save the cookies to a **readable text file**
- Copy cookie** information into the clipboard
- Automatically **refresh the cookies** list when a website sends you a cookie
- Display the cookies** of other users and from other computers
- Open the **IECookiesView utility** directly from Internet Explorer toolbar
- Change the content of a cookie
- Export cookies** to Netscape/Mozilla cookies file
- Block specific websites** from using cookies

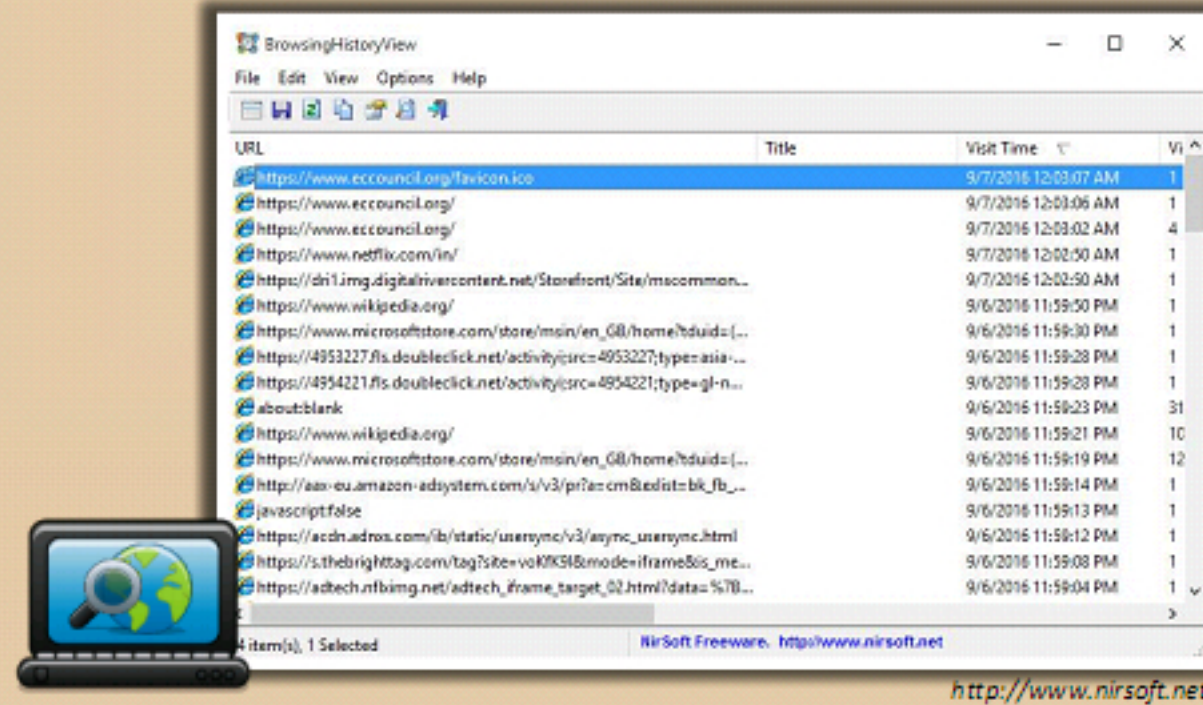
<http://www.nirsoft.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

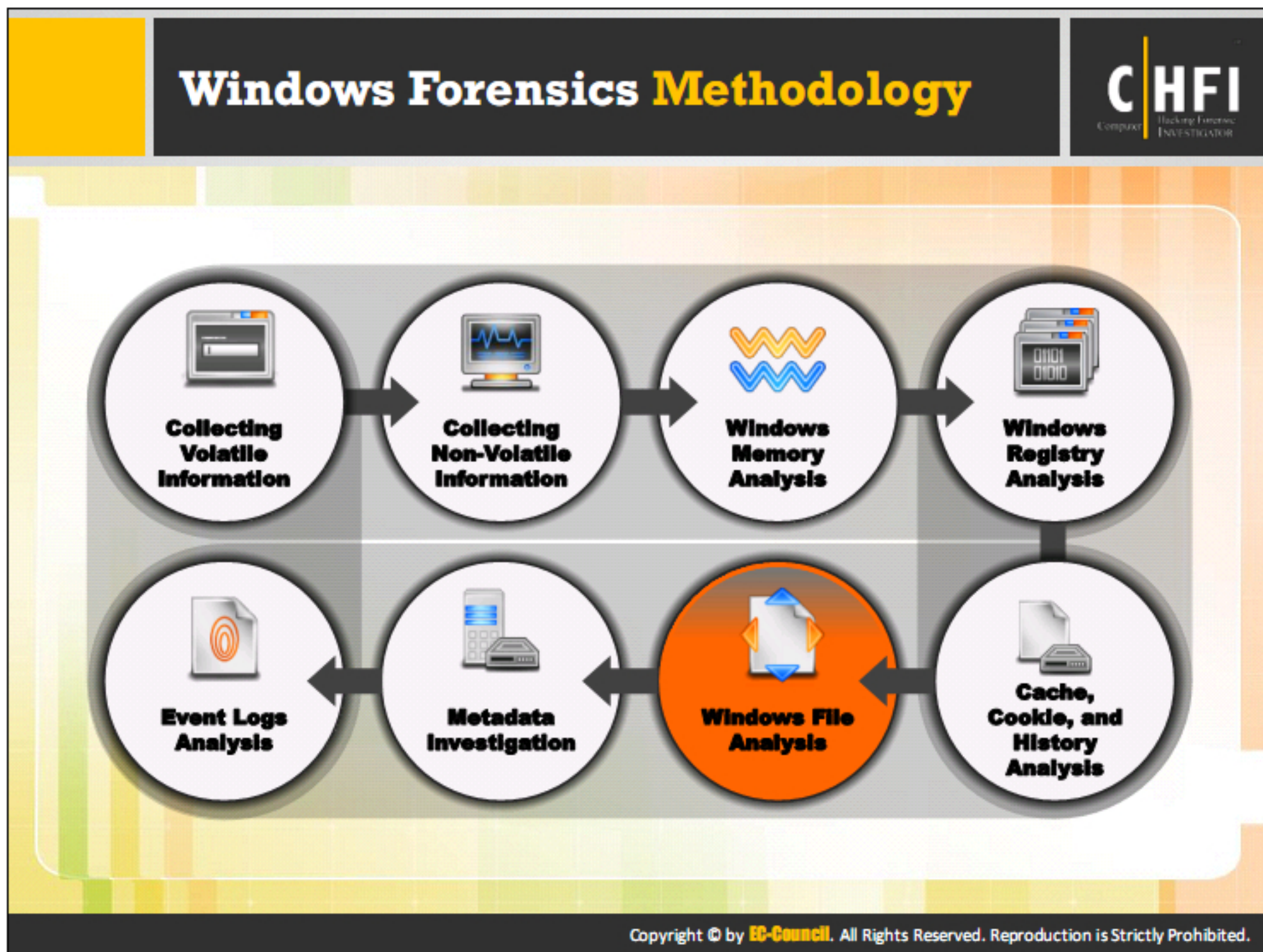
Analysis Tool: BrowsingHistoryView








- BrowsingHistoryView reads history data and **displays the browsing history** in one table
- It allows users to view the browsing history of **all user profiles in a running system**
- The information in the browsing history table includes **Visited URL, Title, Visit Time, Visit Count, Web browser and User Profile**
- Another specialty the extraction of the browsing history from **external hard drive**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.




Windows uses special files to store the data to operate in-built functions such as print, store, restore, etc. Analyzing these files will help investigators find the functions victim or attacker used, and define timeline of events easily.

System Restore Points (Rp.log Files)		CHFI Computer Hacking Forensic Investigator
01	<ul style="list-style-type: none"> Rp.log is the restore point log file located within the restore point (RPxx) directory 	
02	<ul style="list-style-type: none"> It includes value indicating the type of the restore point; a descriptive name for the restore point creation event, and the 64-bit FILETIME object indicating when the restore point was created 	
03	<ul style="list-style-type: none"> Description of the restore point can be useful for information regarding the installation or removal of an application 	
04	<ul style="list-style-type: none"> System restore points are created when applications and unsigned drivers are installed, when an auto update installation and a restore operation are performed 	
05	<ul style="list-style-type: none"> Description of the event that caused the restore point creation is written to the rp.log file, it helps the investigator to notice the date when the application was installed or removed 	
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.		


System Restore Points (Change.log.x Files)		CHFI Computer Hacking Forensic Investigator
1	<ul style="list-style-type: none"> Key system and application files are continuously monitored to restore the system to a particular state 	
2	<ul style="list-style-type: none"> File changes are recorded in the change.log files, which are located in the restore point directories 	
3	<ul style="list-style-type: none"> Changes to the monitored files are detected by the restore point file system driver, the original filename is entered into the change.log file along with sequence number, type of change occurred, etc. 	
4	<ul style="list-style-type: none"> Monitored file is preserved and copied to the restore point directory and renamed to the format Axxxxxxx.ext, where x represents a sequence number and .ext is the file's original extension 	
5	<ul style="list-style-type: none"> First change.log file is appended with a sequence number and a new change.log file is created when the system is restarted 	
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.		

Prefetch Files




1

When a user installs an application, runs it, and deletes it, traces of that application can be found in Prefetch directory




2

DWORD value at the offset 144 within the file corresponds to the number of times the application is launched




3

DWORD value at the offset 120 within the file corresponds to the last time of the application run, this value is stored in UTC format




4

Information from .pf file can be correlated with the Registry or Event Log information to determine who was logged on to the system, who was running which applications, etc.




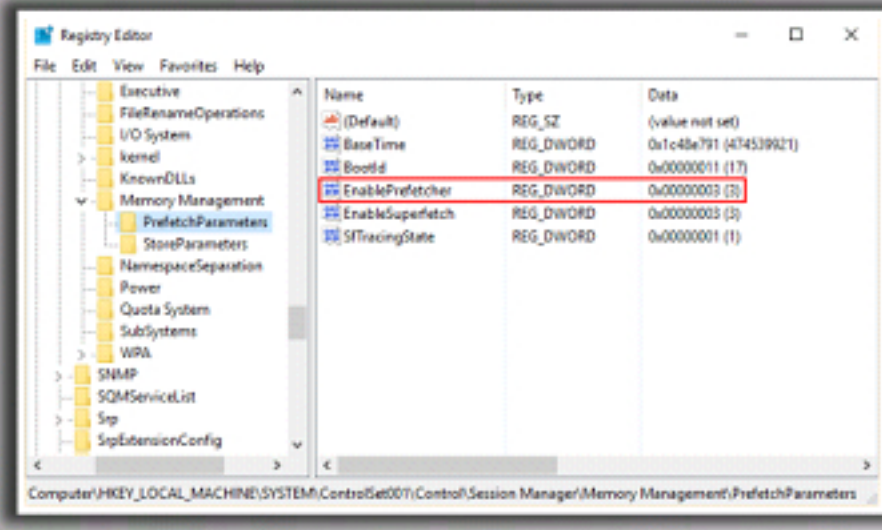
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Prefetch Files (Cont'd)



- Prefetching is to improve system performance
- During boot prefetching, the Cache Manager checks hard page faults and soft page faults
- During application prefetching, the Cache Manager monitors the first 10 seconds after the process is started
- Once the data is processed, it is written to a .pf file in the **Windows\Prefetch** directory
- Prefetching is controlled by the Registry key:
`HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00x\Control\Session Manager\Memory Management\PrefetchParameters`






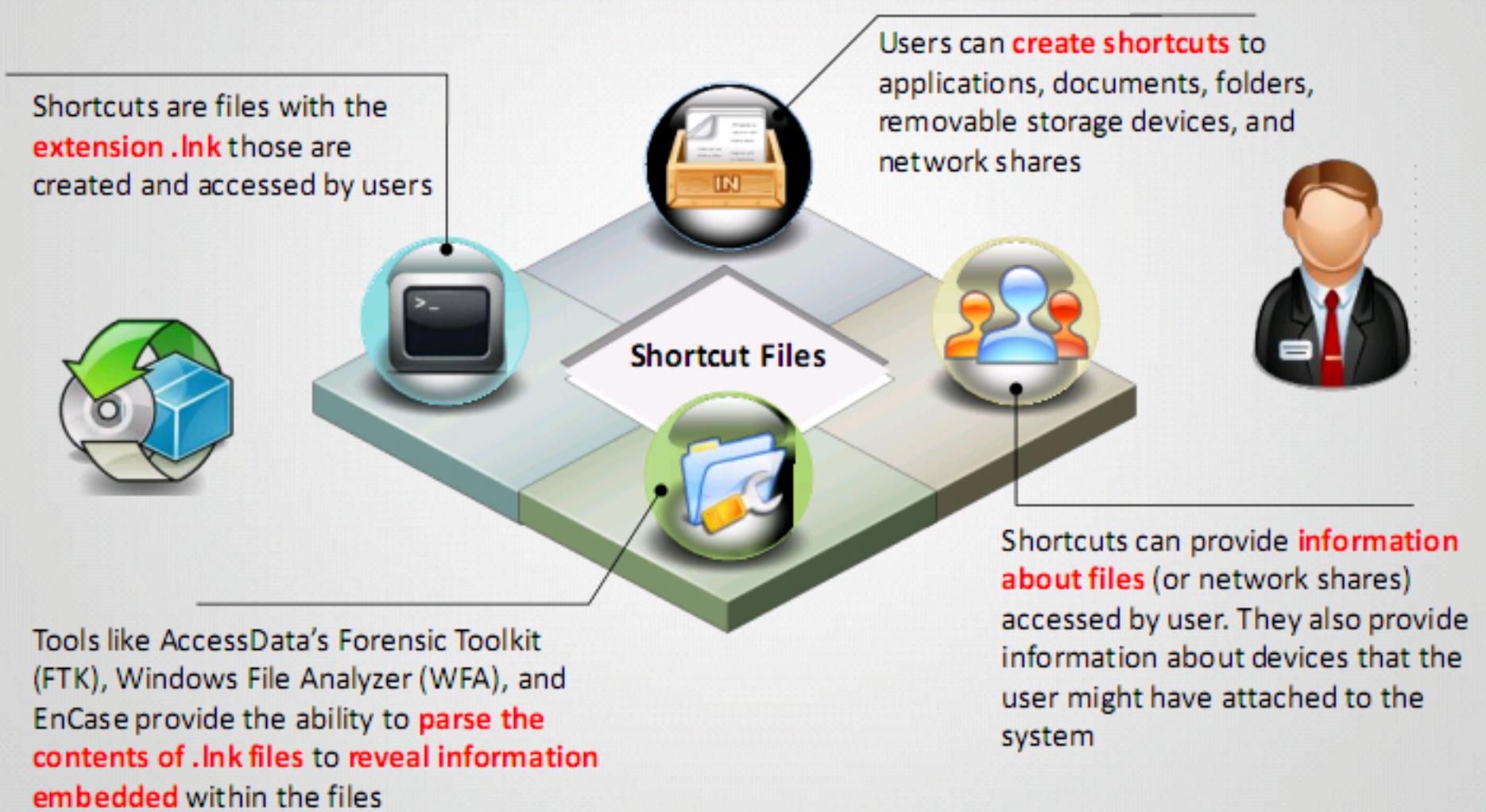
- The data associated with value **EnablePrefetcher** tells which form of prefetching the system uses:

- 0: Prefetching is disabled
- 1: Application prefetching is enabled
- 2: Boot prefetching is enabled
- 3: Both application and boot prefetching are enabled

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Shortcut Files





Shortcuts are files with the **extension .lnk** those are created and accessed by users


Users can **create shortcuts** to applications, documents, folders, removable storage devices, and network shares


Tools like AccessData's Forensic Toolkit (FTK), Windows File Analyzer (WFA), and EnCase provide the ability to **parse the contents of .lnk files** to **reveal information embedded** within the files

Shortcuts can provide **information about files** (or network shares) accessed by user. They also provide information about devices that the user might have attached to the system

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Image Files






The **metadata** present in a JPEG image file depends largely on the application that created or modified it


For e.g., digital cameras embed exchangeable image file format (Exif) information in images, which can include the model and manufacturer of the camera, and can even store thumbnails or audio information



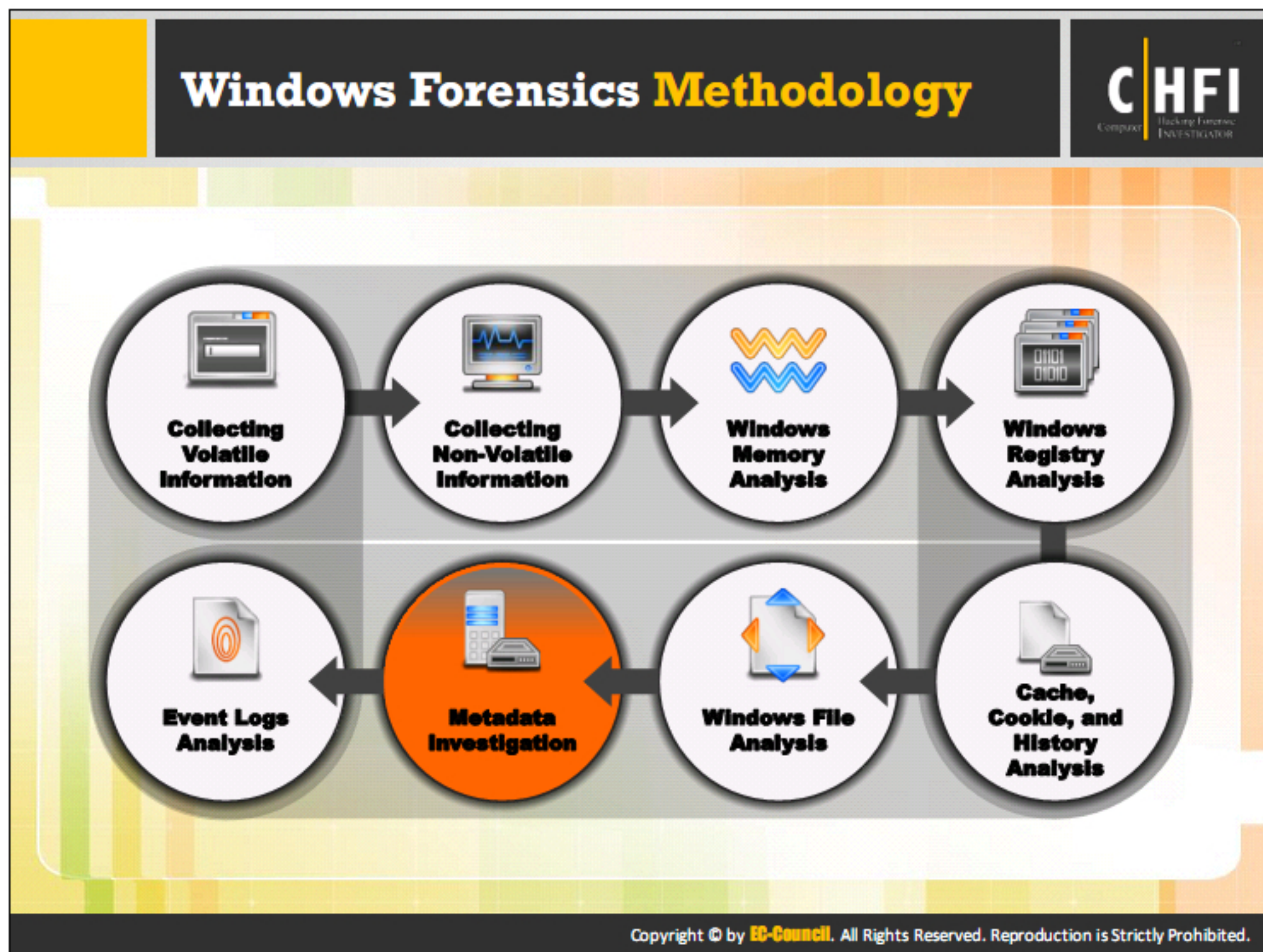


You can use tools such as **Exiv2**, **IrfanView**, and the **Image::MetaData::JPEG** Perl module to view, retrieve, and in some cases modify the metadata embedded in JPEG image files

ProDiscover displays **EXIF** (Exchangeable Image File Format) data found in a JPEG image




Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



Metadata is the information related to the data stored on the system or a device. It contains details such as type of file, time of creation and modification, location, etc. Investigators can extract metadata to find the internal details of any file or application.

Understanding Metadata



- Metadata is data about data. It describes various characteristics of data, including when and by whom it was created, accessed, or modified
- Because it is not normally seen, users can inadvertently share confidential information when sending or providing files in electronic form
- Examples of metadata:**
 - Organization name
 - Author name
 - Computer name
 - Network name
 - Hidden text or cells
 - Document versions
 - Template information
 - Personalized views
 - Non-visible portions of embedded OLE objects
- It is important to collect metadata, as it provides information about the following:
 - Hidden information** about the document
 - Hidden, deleted, or obscured data
 - Correlated documents** from different sources
- The investigator can use tools such as **Metadata Assistant**, **Paraben P2 Commander**, **Metashield Analyzer**, etc. to analyze metadata

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Metadata is structured data, which gives information about certain characteristics of electronic data, including the time and the person that created, accessed, and modified the data. It cannot be seen without using special applications, and users can inadvertently share confidential information when sending or providing files in electronic forms. Examples of metadata include:

- Organization name
- Author name
- Computer name
- Network name
- Hidden text or cells
- Document versions
- Template information
- Personalized views
- Non-visible portions of embedded OLE objects

It is important to collect the data, as it provides information about:


- Hidden data about the document
- Who tried to hide, delete, or obscure the data
- Correlated documents from different sources

Choose the metadata to include in this template:


▼	▼ IPTC Core	▲
<input checked="" type="checkbox"/>	Creator	:
<input checked="" type="checkbox"/>	Creator: Job Title	:
<input type="checkbox"/>	Creator: Address	:
<input checked="" type="checkbox"/>	Creator: City	:
<input checked="" type="checkbox"/>	Creator: State/Province	:
<input checked="" type="checkbox"/>	Creator: Postal Code	:
<input checked="" type="checkbox"/>	Creator: Country	:
<input checked="" type="checkbox"/>	Creator: Phone(s)	:
<input checked="" type="checkbox"/>	Creator: Email(s)	:
<input checked="" type="checkbox"/>	Creator: Website(s)	:
<input type="checkbox"/>	Headline	:
<input type="checkbox"/>	Description	:
<input type="checkbox"/>	Keywords	:
<input type="checkbox"/>	IPTC Subject Code	:
<input type="checkbox"/>	Description Writer	:
<input type="checkbox"/>	Date Created	:
<input type="checkbox"/>	Intellectual Genre	:
<input type="checkbox"/>	IPTC Scene	:
<input type="checkbox"/>	Location	:
<input type="checkbox"/>	City	:
<input type="checkbox"/>	State/Province	:
<input type="checkbox"/>	Country	:
<input type="checkbox"/>	ISO Country Code	:
<input type="checkbox"/>	Title	:
<input type="checkbox"/>	Job Identifier	:
<input type="checkbox"/>	Instructions	:
<input type="checkbox"/>	Provider	:
<input type="checkbox"/>	Source	:
<input checked="" type="checkbox"/>	Copyright Notice	:
<input checked="" type="checkbox"/>	Rights Usage Terms	:

FIGURE 6.4: Metadata selection form

Metadata in Different File Systems



- The most commonly known metadata about files on Windows systems are the **file MAC times**; MAC stands for **modified**, **accessed**, and **created**
- The MAC times are **time stamps** that refer to the time at which the file was last modified, last accessed, and originally created



MAC times are managed by the OS depending on the file system used

- On the **FAT file system**, times are stored based on the **local time** of the computer system
- NTFS file system** stores MAC times in **Coordinated Universal Time (UTC)** format


Investigate the way the **timestamps are displayed**, based on various move and copy actions

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.




The most commonly known metadata about files on Windows systems are the file MAC times. MAC stands for modified, accessed, and created. The MAC times are timestamps that refer to the time at which the file was last modified in some way (data was either added to the file or removed from it), the time when it was last accessed (when the file was last opened), and when the file was originally created.

On the FAT file system, these timings are recorded based on the local time of the computer system, whereas the NTFS file system stores MAC times in Coordinated Universal Time (UTC) format, which is analogous to Greenwich Mean Time (GMT).

Metadata in Different File Systems (Cont'd)



How time stamps are displayed and changed in the FAT 16 and NTFS file systems is shown below

FAT 16 file system	NTFS file system
 <ul style="list-style-type: none">Copy myfile.txt from C:\ to C:\subdir on the same file system (FAT 16) Myfile.txt keeps the same modification date, but the creation date is updated to the current date and timeMove myfile.txt from C:\ to C:\subdir on the same file system (FAT 16) Myfile.txt keeps the same modification and creation datesCopy myfile.txt from a FAT16 partition to an NTFS partition Myfile.txt keeps the same modification date, but the creation date is updated to the current date and timeMove myfile.txt from a FAT16 partition to an NTFS partition Myfile.txt keeps the same modification and creation dates	 <ul style="list-style-type: none">Copy myfile.txt from C:\ to C:\subdir on the same file system (NTFS) Myfile.txt keeps the same modification date, but the creation date is updated to the current date and timeMove myfile.txt from C:\ to C:\subdir on the same file system (NTFS) Myfile.txt keeps the same modification and creation dates 

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Another aspect of file and directory MAC times that interest an investigator are - the way the timestamps are displayed, based on various move and copy actions.

FAT 16 file system:

- Copy myfile.txt from C:\ to C:\subdir – Myfile.txt keeps the same modification date, but the creation date is updated to the current date and time.
- Move myfile.txt from C:\ to C:\subdir – Myfile.txt keeps the same modification and creation dates.
- Copy myfile.txt from a FAT16 partition to an NTFS partition – Myfile.txt keeps the same modification date, but the creation date is updated to the current date and time.
- Move myfile.txt from a FAT16 partition to an NTFS partition – Myfile.txt keeps the same modification and creation dates.

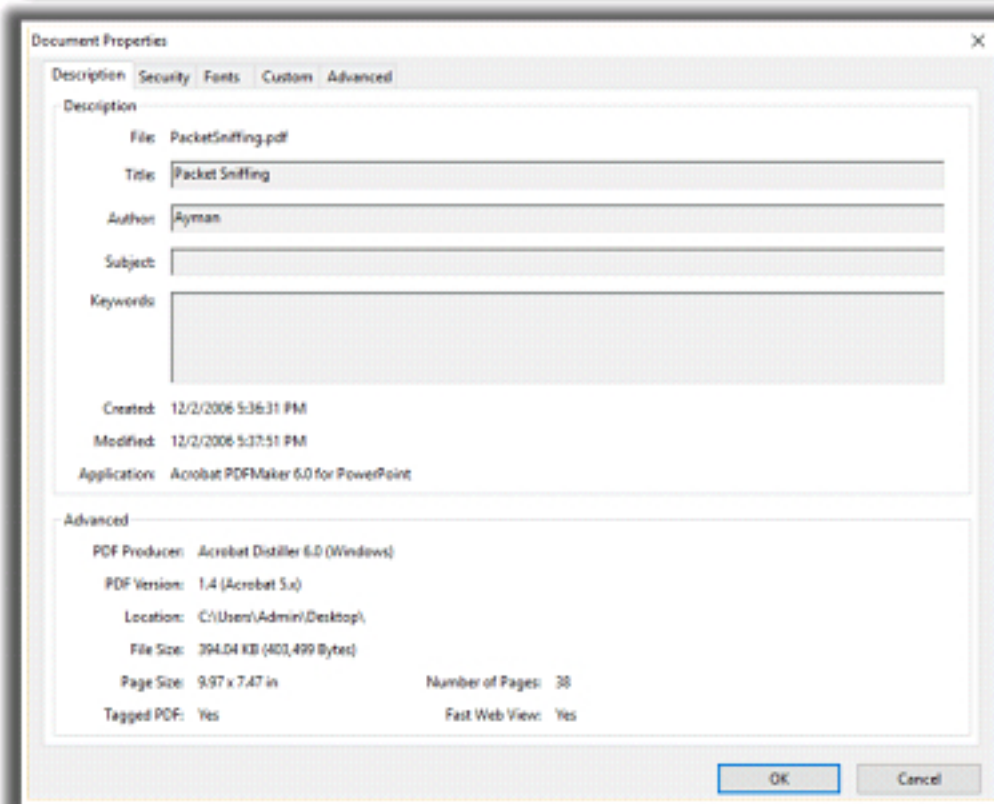
NTFS file system:

- Copy myfile.txt from C:\ to C:\subdir – Myfile.txt keeps the same modification date, but the creation date is updated to the current date and time.
- Move myfile.txt from C:\ to C:\subdir – Myfile.txt keeps the same modification and creation dates.

Metadata in PDF Files



- Portable document format (PDF) files can also contain metadata such as name of the author, the date when file was created, and the application used to create the PDF file
- Often, the metadata can show that the PDF file was created on a Mac or that the PDF file was created by converting a Word document to PDF format
- You can use the Perl scripts `pdfmeta.pl` and `pdfdmp.pl` to extract metadata from PDF files



To view PDF metadata, open it with Adobe Acrobat Reader


In the **File** menu, click **Properties...**



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

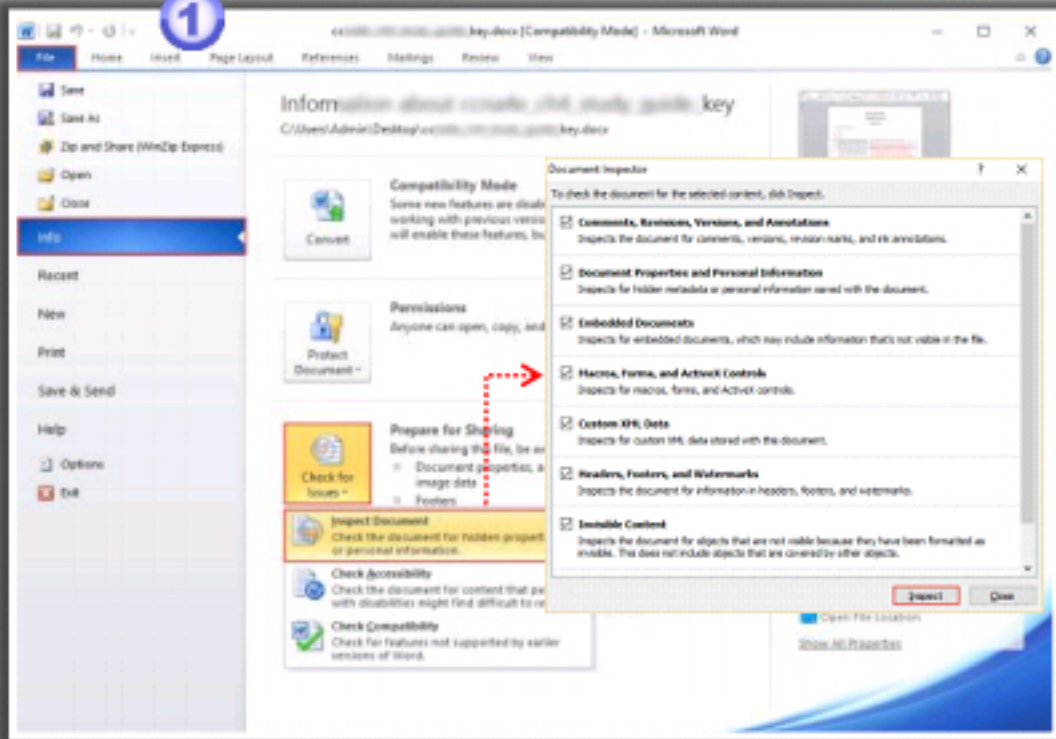
Portable Document Format (PDF) files can contain metadata such as the name of the author, the date that the file was created, and the application used to create that file. The metadata shows that the PDF file was created on Mac or it was created by converting a Word document to PDF format. The `pdfmeta.pl` and `pdfdmp.pl` scripts can be used to extract metadata from PDF files. Another way to retrieve metadata is to open the file in Adobe Reader and click **File** → **Properties**. The Description tab of the Properties dialog box contains all the available metadata.

Metadata in Word Documents

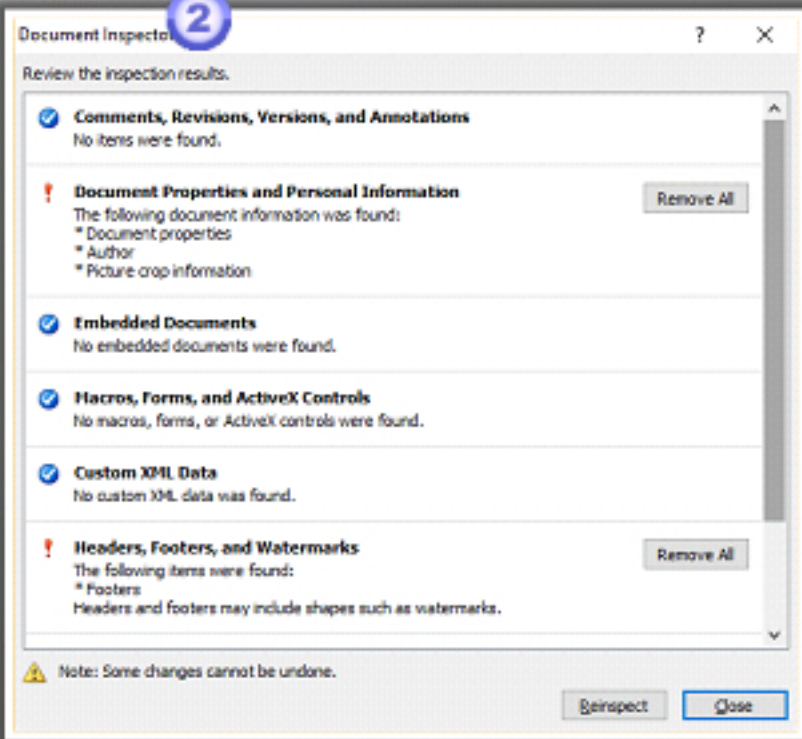


- Word documents are compound documents, based on Object Linking and Embedding (OLE) technology that defines the file structure
- Word documents can maintain not only past revisions but also a list of up to the last 10 authors to edit the file
- You can use the Perl scripts **wmd.pl** and **oledmp.pl** to list the OLE streams embedded in a Word document
- To view metadata in Word 2010, click on the **File** tab → **Info** option
- Click **Check for Issues** → **Inspect Document**
- Select the content to view and click the **Inspect** button

1



2



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


Word documents are compound documents, based on the Object Linking and Embedding (OLE) technology that defines a “file structure within a file.” Besides formatting information, Word documents can contain quite a bit of additional information that is not visible to the user, depending on the user’s view of the document.

Word documents can maintain not only past revisions but also a list of up to the last 10 authors who edited a file. This has posed an information disclosure risk to individuals and organizations. Perl scripts **wmd.pl** and **oledmp.pl** are used to list the OLE streams and trash bins embedded in a Word document.

Metadata in MSWord 2010 can be viewed by following the below mentioned steps:

- Click on the **File** tab → **Info** option
- Click **Check for Issues** → **Inspect Document**
- Select the content to view and click the **Inspect** button

Metadata Analysis Tool: Metashield Analyzer



Select file

Enter file path or upload file, Report.docx

Analyze

These are the metadata found:

Data relating to dates

Creation Date: 12/14/2010 4:24:00 PM
Modification Date: 12/14/2010 4:24:00 PM
Print Date: 12/14/2010 5:10:00 AM

Metadata

Title: Contemporary Letter
Application: Microsoft Office 2007
Category: Letter
Times Edited: 2
Edition Time: 1 Minutes

Users found

LastModifiedBy: Office of Information Technology
Creator: Pouts

Paths found

Path: http://www.professionalequipment.com/industry-science-to-multi-gas-monitor-le-o2-co-10104507-11100-multi-gas-meters/
Path: http://www.robotshop.com/
Path: http://www.professionalequipment.com/honeywell-lumidon-micromax-pro-multi-gas-monitor-le-o2-co-h2-mpro-48bcd-multi-gas-meters/
Path: http://www.air.dnr.state.ga.us/information/
Path: http://www.roanoke.com/news/special/wb/
Path: http://www.drillspot.com/products/330374/
Path: http://store.robot.com/category/
Path: http://users.ece.gatech.edu/~hamblen/48SIX/F09/PKQ/FireFinger_Robot/
Path: http://inspectusa.com/
Path: http://www.google.com/products/
Path: http://compare.ebay.com/like/
Path: http://www.logitech.com/en-us/webcam-communications/webcams/devices/
Path: http://www.compactpc.com/bv/
Path: http://www.cdnstores.com/asp/

Emails found

Email: eric@hawaii.edu
Email: Eric.Hamblen@hawaii.edu
Email: ryl@hawaii.edu
Email: hamblen@hawaii.edu

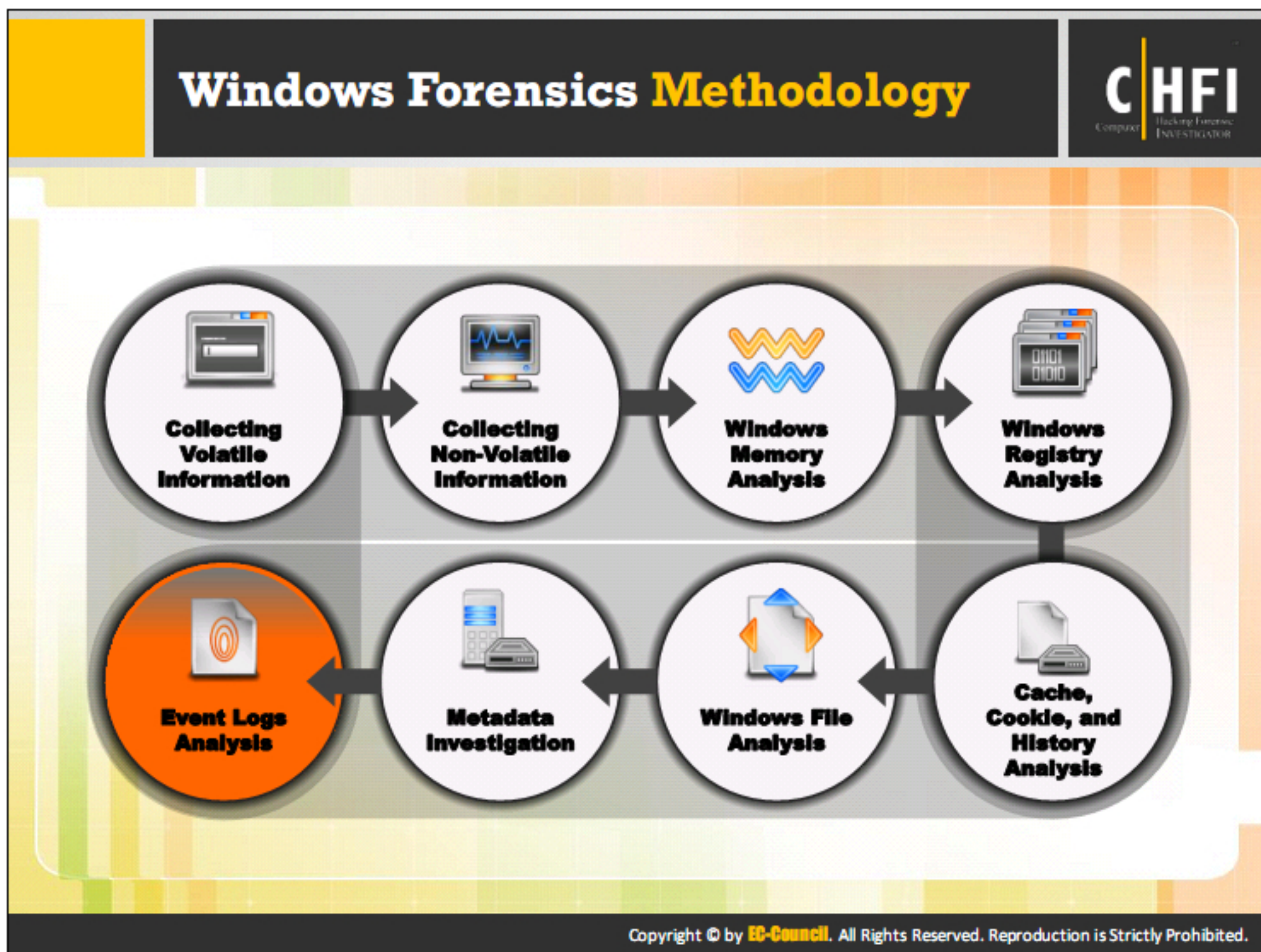
Metashield Analyzer is an **online service** that allows to **analyze the metadata** contained in files

<https://www.elevenpaths.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Metashield Analyzer is an online tool to analyze the metadata contained in a file. This tool reveals the details like Creation and Modification date, Users found and the name of the application worked on, Number of times Edited and the paths found. A file can be analyzed by using the following procedure.

- Click **Select File** → select the required file.
- Click **Analyze**, accept the Terms and conditions in the Pop-up.
- Click on **Analyze** to view the output i.e. the Metadata of the file.



Logs are the sequential records of events that have occurred or performed over a system. All the operating systems have the ability to store these records. Investigators can build timeline based on these logs and find exact time and location of attack.

Operating systems regularly conduct audit of the contents and files in order to look for discrepancies. These files store the data regarding the previous state of a system. Investigators can extract the state data and compare it with current state to find the attack vectors

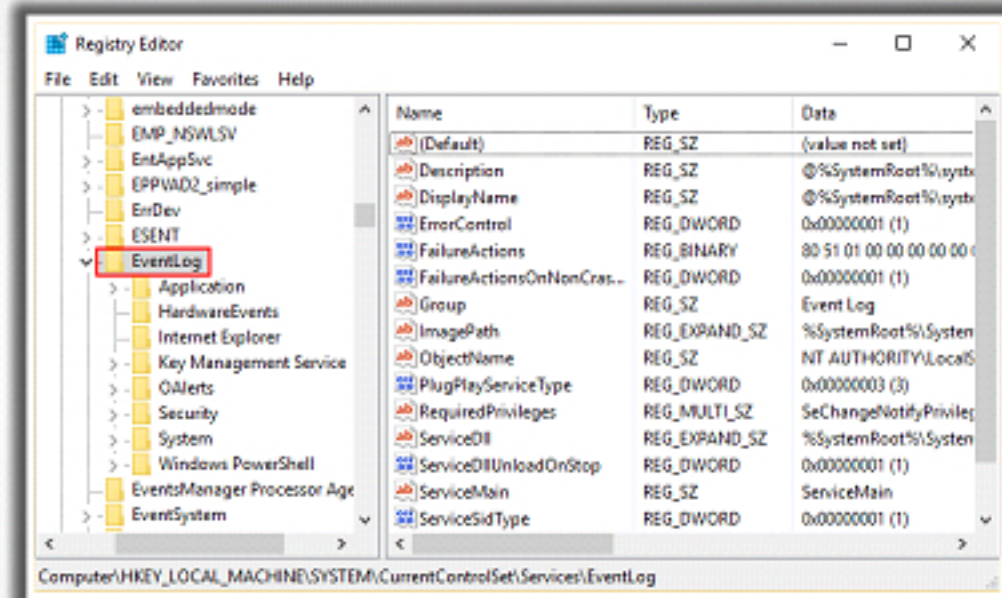
This section will discuss the process of analyzing event logs of a windows based system in a forensically sound manner. It is important for investigators to know the proper way of analyzing different system logs.

Forensics tools help investigators by simplifying and speeding their work. This section of the document will help in understanding different forensics tools their purpose and the ways to use them.

Understanding Events



- Event logs **record** a variety of day-to-day **events** that occur on the Windows systems
- Some events are recorded by default and some audit configurations are maintained in the **PolAdEvt** Registry key
- The **Registry** key which maintains the Event log configuration:
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\<Event Log>**



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Event logs can be very helpful to the investigators to find data related to the suspected incident. The event log information is dependent on the particular audit policies implemented. It means that the event logs record only the information mandated in the audit policies. Using these logs, the investigator can map various activities performed on the system by the users, their IP addresses, or groups. These activities can include number of failed logins, high number of logins etc. This can assist the investigator to trace the attacker.

Types of Logon Events



Logon Type	Title	Description
2	Interactive	A user logged on to this computer
3	Network	A user or computer logged on to this computer from the network
4	Batch	Batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention
5	Service	A service was started by the Service Control Manager
7	Unlock	This workstation was unlocked
8	NetworkCleartext	A user logged on to this computer from the network. The user's password was passed to the authentication package in its unhashed form.
9	NewCredentials	A caller cloned its current token and specified new credentials for outbound connections
10	RemoteInteractive	A user logged on to this computer remotely using Terminal Services or Remote Desktop
11	CachedInteractive	A user logged on to this computer with network credentials that were stored locally on the computer

<https://technet.microsoft.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Event Log File Format



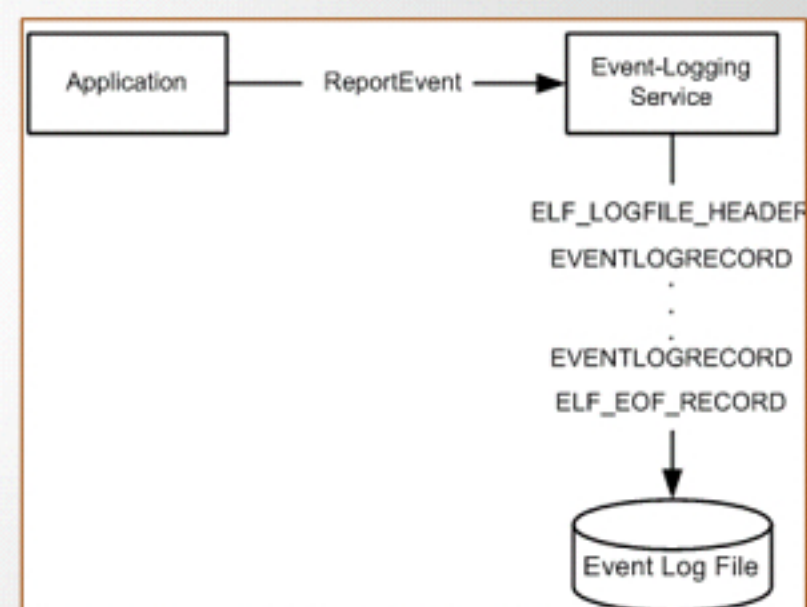
Each event log consists of a:

- Header of fixed size (represented by the **ELF_LOGFILE_HEADER** structure)
- Variable number of event records (represented by **EVENTLOGRECORD** structures)
- End-of-file record (represented by the **ELF_EOF_RECORD** structure)

When the event log is created and updated, both the **ELF_LOGFILE_HEADER** structure and the **ELF_EOF_RECORD** structure are written to it

In the diagram, an application calls the **ReportEvent** function to write an entry to the log file

The system then passes the parameters to the event-logging service, which uses the information to write an **EVENTLOGRECORD** structure to the event log file



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



We can organize the event records in two ways; one is through non-wrapping and the other is through wrapping.

Non-wrapping

As represented in the slide, in non-wrapping event record organization, the oldest record exists after event log header, and the new record is placed last. This method is implemented for maximum log sizes. This size depends on the configured size value or number of system resources. Wrapping method is applied when the log size limit is crossed.

Wrapping

As represented in the slide, in wrapping event record organization, the oldest record is 102 instead of 1. The oldest record and ELF_EOF_RECORD have some empty space between them, in order to make place for the new records. The event log file size has a limit and when this file size exceeds, the file records are wrapped. When wrapping begins the last record of the file will be divided into two.

ELF_LOGFILE_HEADER Structure



The event-logging service adds the **ELF_LOGFILE_HEADER** at the start of the event log, which describes information about the event log

Members	Description
HeaderSize	The size of the header structure, which is always 0x30
Signature	The signature is always 0x54c664c, which is ASCII for eLFL
MajorVersion	The major version number of the event log and is always set to 1
MinorVersion	The minor version number of the event log and is always set to 1
StartOffset	The offset to the oldest record in the event log
EndOffset	The offset to the ELF_EOF_RECORD in the event log
CurrentRecordNumber	The number of the next record that will be added to the event log
OldestRecordNumber	The number of the oldest record in the event log. Its value is set to zero for an empty file.
MaxSize	The maximum size, in bytes, of the event log. It is defined when the event log is created
Flags	The status of the event log. It could be one of the four values:
Retention	The retention value of the file when it is created
EndHeaderSize	The signature is always 0x54c664c, which is ASCII for eLFL

Value	Meaning
ELF_LOGFILE_HEADER_DIRTY0x0001	Indicates that records have been written to an event log, but the event log file has not been properly closed
ELF_LOGFILE_HEADER_WRAP0x0002	Indicates that records in the event log have wrapped
ELF_LOGFILE_LOGFULL_WRITTEN0x0004	Indicates that the most recent write attempt failed due to insufficient space
ELF_LOGFILE_ARCHIVE_SET0x0008	Indicates that the archive attribute has been set for the file. Normal file APIs can also be used to determine the value of this flag

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EventLogRecord Structure



The **EventLogRecord** structure contains information on a single event

Component	Size	Description
Length	4 bytes	Size in bytes of the structure
Reserved	4 bytes	Serves as a signature for the structure
Record Number	4 bytes	It is mapped directly from the record ID. The record ID is an unsigned int64 (an 8 byte number) that the server reads from the file and converts to an unsigned integer (a 4 byte number) when assigning the value to the RecordNumber field in the EVENTLOGRECORD structure
TimeGenerated	4 bytes	Time when the event was generated. The time MUST be expressed as the number of seconds since 00:00:00 on January 1, 1970 (UTC). This value is supplied by the event source.
TimeWritten	4 bytes	Time when the event was written. The time MUST be expressed as the number of seconds since 00:00:00 on January 1, 1970 (UTC). This value is the time the event was written to the event log
EventID	4 bytes	EventID generated by the event source
EventType	2 bytes	Type of the event
NumStrings	2 bytes	Number of strings in the Strings field. Its value must be between 1 and 256
EventCategory	2 bytes	Event category

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The event record structure allows organization of incomplete records present in the unallocated space. The magic number helps to search these records in the unallocated space. The event record consists of a 56 byte header which can help to reconstruct parts of the event record, if the record is not available.

Length

The length of the event record indicates the event record size in bytes.

NumStrings

This indicates the number of the strings that are in the log. The user gets the message after these strings are merged in the message.

EventID

Event ID or event identifier is used to identify an event. This ID depends on the event source. Every event source can define the value of its event ID. The event ID and the source name together are used to find a text in the message file for the event source.

EventType

Events are of five kinds namely, error event, warning event, information, success audit and failure audit. Every event type has significance and provides specific details of the event. When an event occurs its respective event type is indicated by the application. An event cannot be of two event types, at a time an event can be only of one type.

- **Error:** It denotes an issue or problem like data loss
- **Warning:** It is an indication of future occurrence of error
- **Information:** This event gives details of the occurrence of a successful operation
- **Success Audit:** This event records a successful audited security access attempt
- **Failure Audit:** This event records a failed audited security access attempt

EventCategory

It indicates the category of an event. Every source of the event defines the value of its event category. Event categories make it easy to organize various events.

EventLogRecord Structure (Cont'd)



Component	Size	Description
ReservedFlags	2 bytes	Specifies whether or not the last string in the Strings field contains well-formed XML. The value 0x0000 indicates that the event does not contain XML and the value 0x8000 indicates that the event contains XML.
ClosingRecordNumber	4 bytes	MUST be set to zero when sent and MUST be ignored on receipt.
StringOffset	4 bytes	This MUST be the offset in bytes from the beginning of the structure to the Strings field. If the Strings field is not present (NumStrings is zero), this can be set to any arbitrary value when sent and MUST be ignored on receipt by the client.
UserSidLength	4 bytes	Size in bytes of the user's security identifier, which is located within the UserSid field. If there is no UserSid field for this event, this field MUST be set to zero.
UserSidOffset	4 bytes	This MUST be the offset in bytes from the beginning of the structure to the UserSid field. If the UserSid field is not present (i.e., if UserSidLength is zero), this can be set to any arbitrary value when sent and MUST be ignored on receipt by the client.
DataLength	4 bytes	This MUST be the size in bytes of the Data field. If the Data field is not used, this field MUST be set to zero.
DataOffset	4 bytes	This MUST be the offset in bytes from the beginning of the structure to the Data field. If the Data field is not present (that is, if DataLength is zero), this can be set to any arbitrary value when sent and MUST be ignored on receipt.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


EventLogRecord Structure (Cont'd)



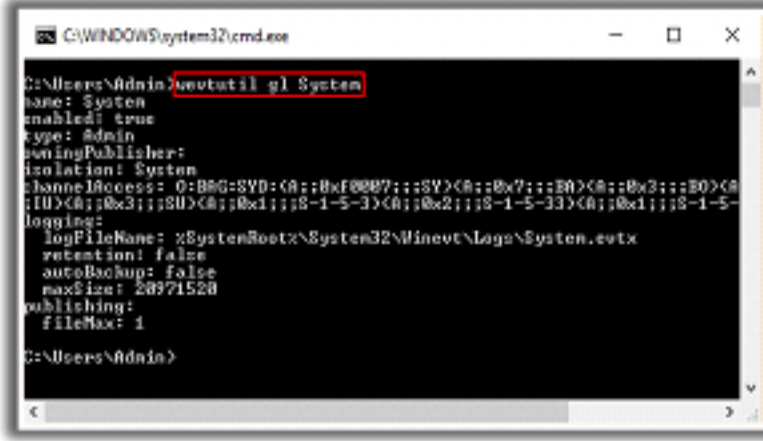
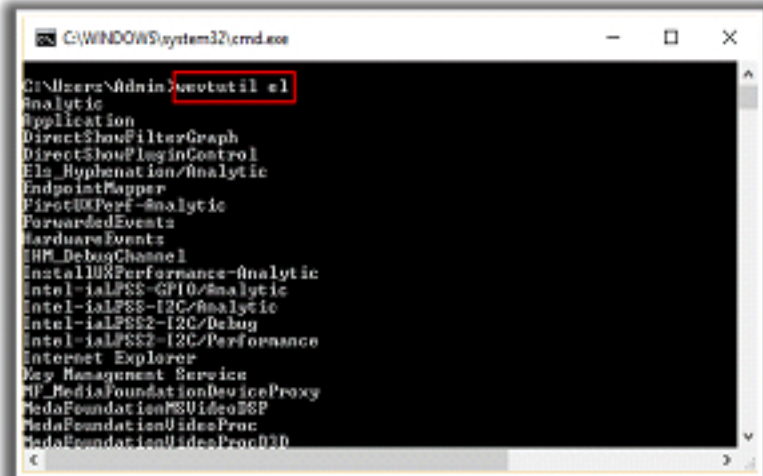
Component	Size	Description
SourceName	Variable	Variable-length null-terminated string that specifies the name of the source that generated the event. The length of this field is calculated by seeking the NULL that terminates the string.
Computername	Variable	Variable-length null-terminated string that assists in identifying the machine that generated the event. This string MUST NOT be interpreted by the protocol, and can be in an arbitrary format.
UserSidPadding	Variable	MUST be zero or more bytes of padding, where the choice of length is implementation dependent. The padding can have any value, and MUST be ignored on receipt.
UserSid	Variable	Current user's security identifier, as defined by the RPC_SID structure. This parameter can be NULL if the security identifier is not required.
Strings	Variable	Zero or more null-terminated strings containing information on the event. The numStrings field contains the number of items in this field.
Data	Variable	Event-specific binary data. This is supplied by the event source, and MUST NOT be interpreted by the protocol. This data is not always present. The DataLength field contains the length of this field. The DataOffset field contains the start of this field.
Padding	Variable	The SourceName, ComputerName, UserSid, Strings, and Data fields can all vary in length. The UserSid, Strings, and Data fields MAY be zero bytes in length. The length of the entire structure up to this point, including these fields, MUST be divisible by 4. Therefore, up to 3 bytes of padding MUST be added to bring the length to a multiple of 4. The padding can have any value, and MUST be ignored on receipt.
Length2	4 bytes	Same value as the Length field specified as the first member. By having two copies, a buffer containing many events can easily be navigated in both directions.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows 10 Event Logs



- In Windows 10, the event logs are saved in **.xml** format
- wevtutil** command can be used to retrieve information about event logs and publishers that is not readily apparent via the Event Viewer user interface
- Command to display a list of available Event Logs on the system:
C:\>wevtutil el
- Command to list configuration information about a specific Event Log:
C:\>wevtutil gl <log name>
- Information displayed by this command is also available in the following key on a Windows 10 system:
HKLM\System\ControlSet00x\Services\EventLog\<log name>




Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Wevtutil


This tool enables you to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, to run queries, and to export, archive, and clear logs.

Source: <https://technet.microsoft.com>

Evaluating Account Management Events



- The account management category of events is used to record changes to accounts and group membership
- This includes:
 - Creation
 - Deletion
 - Disabling of accounts
 - Modifying which accounts belong to which groups
 - Account lockouts
 - Account reactivations



- If auditing of the account management events has been activated, it helps investigators to identify activities performed by an attacker on gaining access to a system
- The description for an account creation or deletion event includes the following information:
 - A Summary of the type of action
 - The account that performed the action is listed in the **Caller User Name** field
 - The account added or removed is shown in the **Member ID** field
 - The affected group is listed as the **Target Account Name**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The account management category of events is used to record the changes in accounts and group membership. This includes creation, deletion, and disabling of accounts; modification of accounts which belong to other groups; and account lockouts and reactivations. Various Event IDs are associated with changes in the accounts.

An account can be a domain account or a local account and can represent a user, computer, or service. Domain account events will be recorded on domain controllers, and events related to local accounts will be recorded on the local computer involved in the operation. These events are recorded regardless of whether the account represents a user, computer, or service. When an account is created, Event ID 624 is recorded. This event shows the name of the newly created account, along with the name of the account that was used to create it. Another event ID 642, gives the information about the changes made to the account.

When reading the description for an event that involves adding or removing an account to or from a group, these rules apply:

- The first line of the description summarizes the type of action.
- The account that performed the action is listed in the Caller User Name field,
- The account added or removed is shown in the Member ID field.
- The group affected is listed as the Target Account Name.

Evaluating Account Management Events (Cont'd)



Event ID	Event Message
4727	A security-enabled global group was created
4728	A member was added to a security-enabled global group
4729	A member was removed from a security-enabled global group
4730	A security-enabled global group was deleted
4731	A security-enabled local group was created
4732	A member was added to a security-enabled local group
4733	A member was removed from a security-enabled local group
4734	A security-enabled local group was deleted
4735	A security-enabled local group was changed
4737	A security-enabled global group was changed
4754	A security-enabled universal group was created
4755	A security-enabled universal group was changed
4756	A member was added to a security-enabled universal group
4757	A member was removed from a security-enabled universal group
4758	A security-enabled universal group was deleted
4764	A group's type was changed

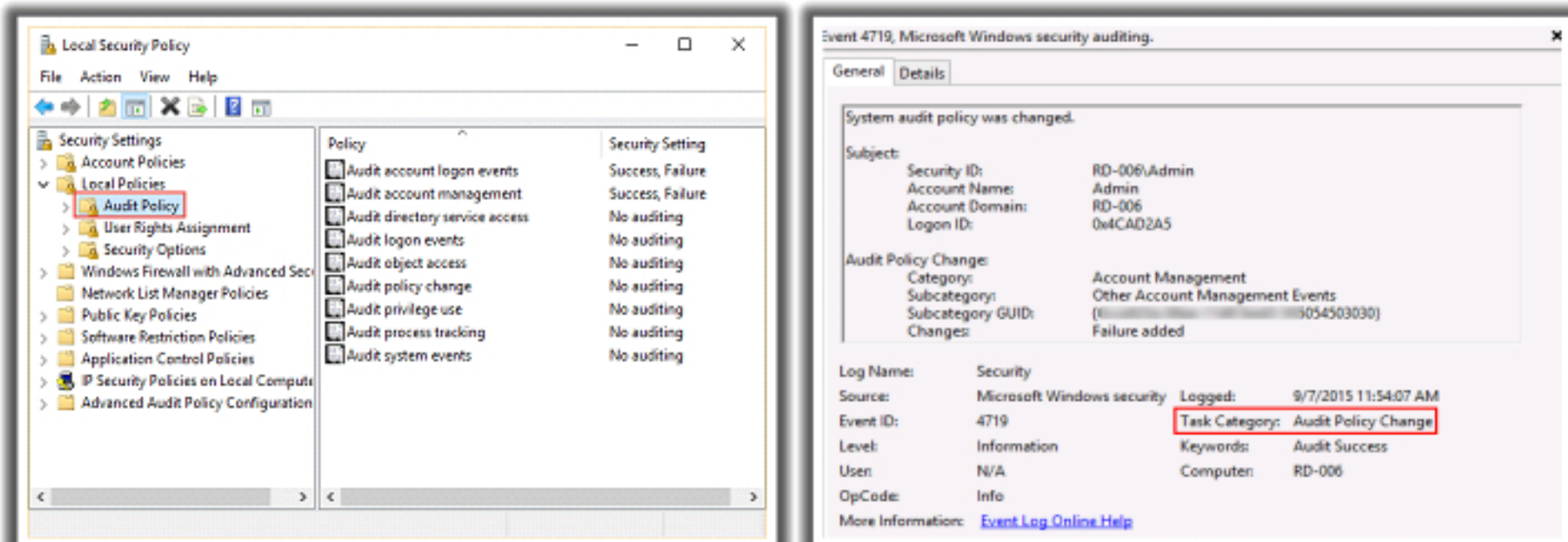
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

In Microsoft Windows, the “Security log” stores data pertaining to login/logout activities or any other events related to security, as specified by the system’s audit policy. Auditing allows System administrators and investigators to configure Windows, in order to record the activities in the Security Log. The security logs play a major role in detecting and investigating the attempted logins, unsuccessful events, and unauthorized events.

Evaluating Account Management Events (Cont'd)



- When a system is compromised, attackers will often attempt to **disable auditing**
- Examining Audit Policy Change** determines whether the OS generates audit events when changes are made to audit policy
- To locate the Audit Policy:
Right-click **Start** → click **Run** → Type **secpol.msc** → press **Enter** → double-click **Local Policies** → click **Audit Policy**




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

When a system is compromised, attackers will frequently attempt to disable auditing. Modifications to the audit policy are recorded in Event ID 612 entries. The + symbols indicate the events that are being audited, whereas the – symbols show the categories which are not being audited. Success and Failure events are being audited for Logon/Logoff, Object Access, and Account Management events. However, nothing is being audited for Privilege Use, Policy Change, System, or Detailed (process) Tracking events. The Event ID 612 entry allows the user to deduce the changes that were made by comparing the old policy to the new policy.

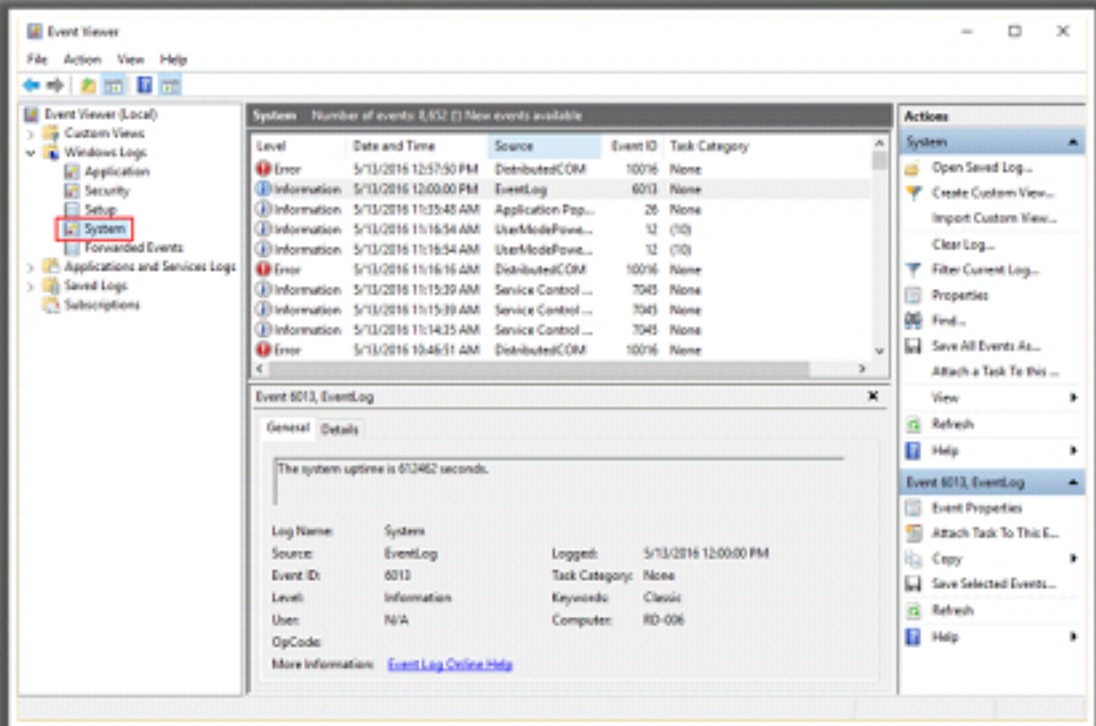
With Group Policy changes set to ON, the domain controller takes precedence over changes made to the local audit policy in an individual computer. Due of this, the attackers may not be able to completely disable auditing. If the attacker disables auditing on a computer that is a member of a domain, the domain's Group Policy audit settings may override that change during the next policy update.

Locate the audit policies by clicking **Start** → **Run**, then typing **secpol.msc** and pressing **Enter**. In the Local Security Policy window, click **Local Policies** → **Audit Policy**.

Examining System Log Entries



- The System log contains events logged by Windows system components
- System log includes:
 - Changes to the OS
 - Changes to the hardware configuration
 - Device driver installation
 - Starting and stopping of services
- To locate the System log entries:
Right-click **Start** → click **Control Panel** → **System and Security** → **Administrative Tools** → double-click **Event Viewer** → click **Windows Logs** → double-click **System**



Log Name	Source	Logged
System	EventLog	5/13/2016 12:00:00 PM
Event ID	Task Category	Level
6013	None	Information
User	OpCode	Keywords
N/A		Classic
		Computer: RD-006

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

System Log records the events relating to the various aspects of system behavior, which includes changes to the operating system, hardware configuration, device driver installation, the starting and stopping of services, and a host of other items of potential investigative interest.

Whenever a service is to be stopped, the Service Control Manager sends a stop signal to the service and simultaneously sends a message (Event ID 7035) to the System event log, advising that the stop signal was sent to a particular service. When the service actually stops, the Service Control Manager again sends a message (Event ID 7036) to the System event log, advising that the service actually stopped.

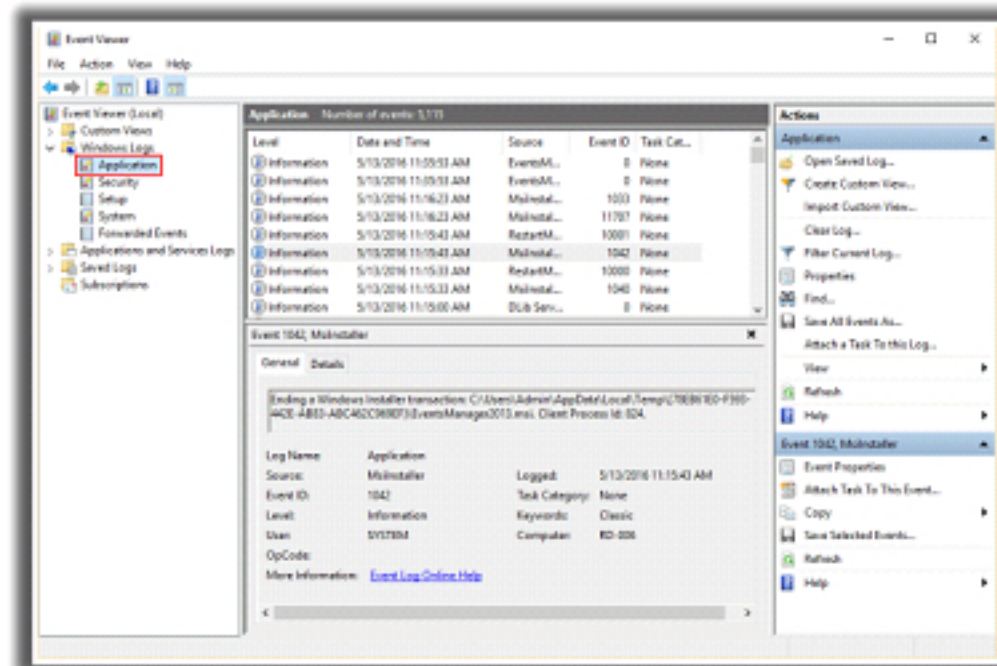
Similarly, if a service is started, the Service Control Manager sends a start control signal to the service and simultaneously sends a message (Event ID 7035) to the System event log advising that the start control signal was sent. When the service starts, the Service Control Manager sends a message (Event ID 7036) to the System event log, advising that the service actually started.

To navigate the System log entries, click **Start** → **Control Panel** → **System and Security** → **Administrative Tools** → double-click **Event Viewer** → click **Windows Logs** → double-click **System**.

Examining Application Log Entries



- The **Application log** contains events logged by applications or programs
- To locate the Application log entries:
 - Right-click **Start** → click **Control Panel** → **System and Security** → **Administrative Tools** → double-click **Event Viewer** → click **Windows Logs** → double-click **Application**
- The VNC application records connections to the VNC server in the **Application log**, with the IP and port from which the connection originated



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Application event log contains messages from both the operating system and various programs. The user can actually use a program from Microsoft called logevent.exe to send custom messages, typically when batch files are run. By default, this program sends messages to Event ID 1 of the Application event log, unless another Event ID is specified.

Many utilities especially anti-virus and other system-protection programs send messages to the Application event log relating to their scanning activities, detection of malware, and so on.

Virtual Network Computing (VNC) is similar to the Windows Remote Desktop feature and allows establishment of remote connections. The VNC application records the information relating to the connections made with the VNC server, with the IP and port information from which the connection originated, in the Application event log.

To navigate to the **Application log entries**, click **Start** → **Control Panel** → **System and Security** → **Administrative Tools** → double-click **Event Viewer** → click **Windows Logs** → double-click **Application**.

Searching with Event Viewer

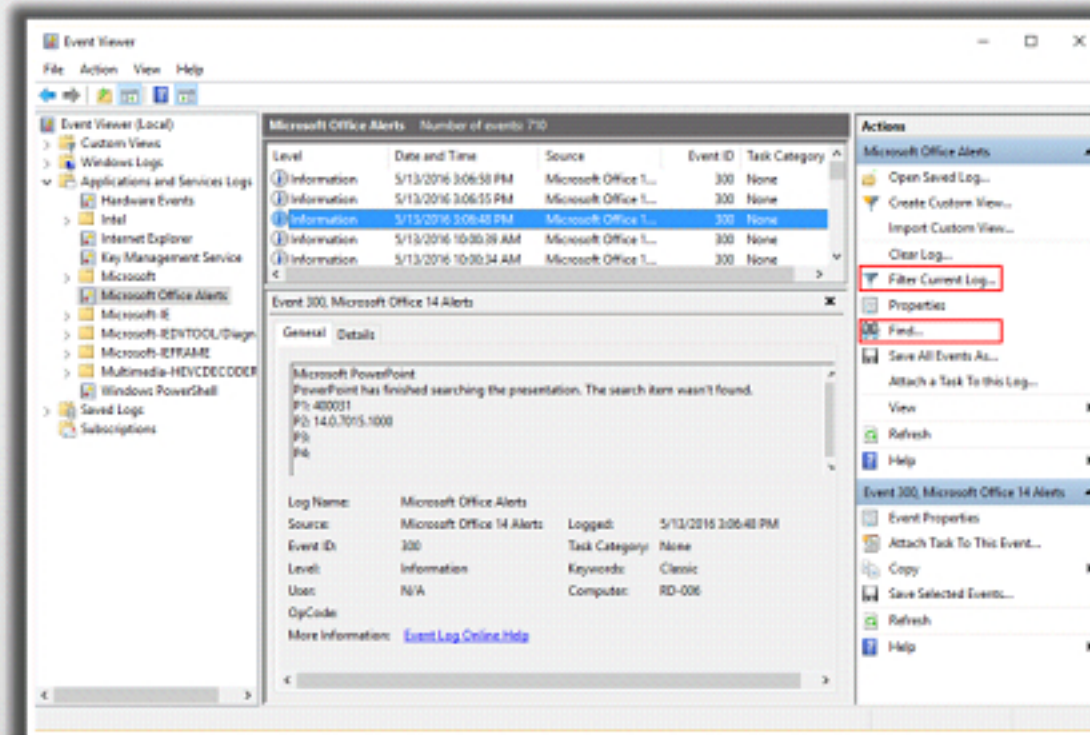


1 The **Filter** feature in the event viewer allows the removal of clutter from the event log display

2 Each log can be independently configured with different filter properties

3 Use **Filter** and **Find** features in Event Viewer, under the **Actions** pane

4 After applying the filter, the Event Viewer will show the log with matching properties



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

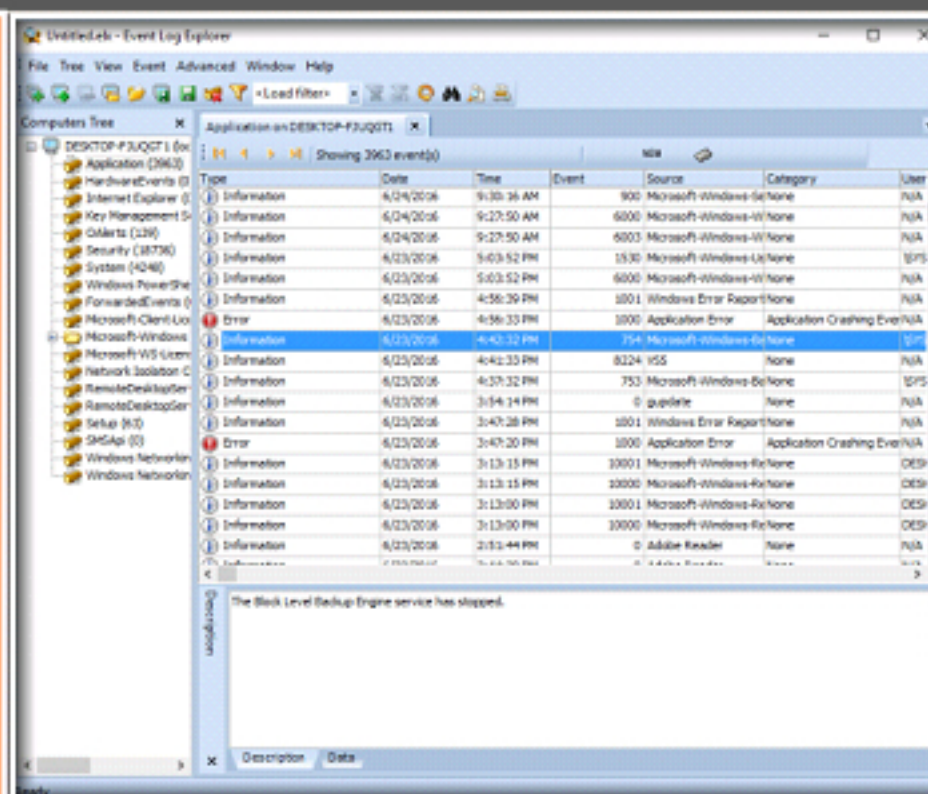
Using Event Log explorer to Examine Log Files



Event Log Explorer helps in viewing, analyzing, and monitoring events recorded in **Windows**

Reasons to use the tool are:

- It helps to keep the processed information within the forensic environment
- It does not rely on the Windows API to process the event logs



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Filter feature in the Event Viewer allows removal of a lot of the clutter from the event log display. Filtering does not modify the event log in any way, but it does change parts of the Event Log Viewer. Filters can be set, reset, or changed without impacting the contents of the event log. To filter the logs, right-click any log type that you want to filter and select Filter Current Log.

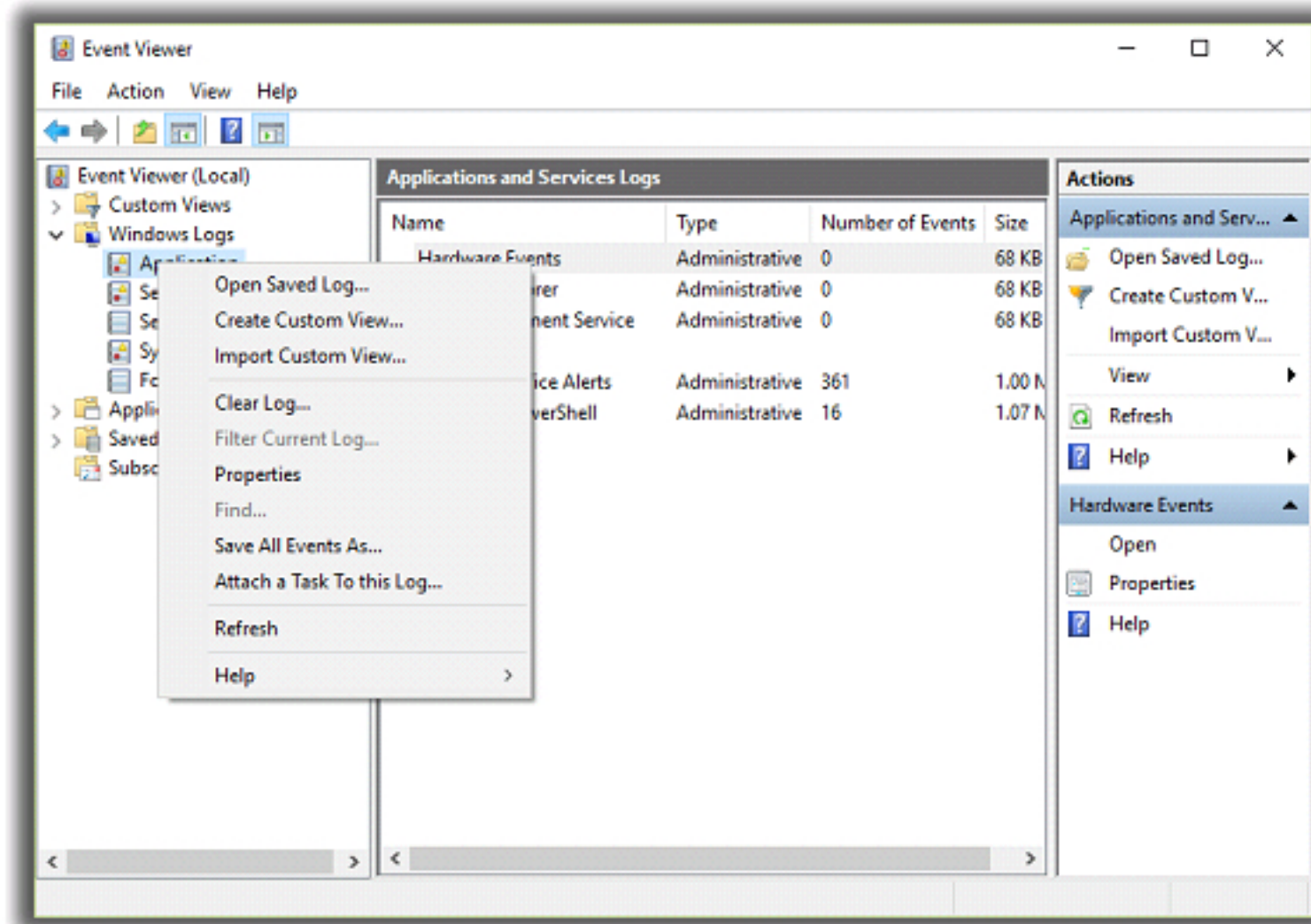


FIGURE 6.5: Event Viewer Tree Pane

In the Filter Current Log wizard, check the Critical, Error, and Warning boxes and click OK to view only failure-related events or logs. You can also filter the events by time with predefined values like Last hour, Last 12 hours, Last 24 hours, Last 7 days, and Last 30 days, by specifying your own time frame or by selecting Custom range from the Logged drop-down list.

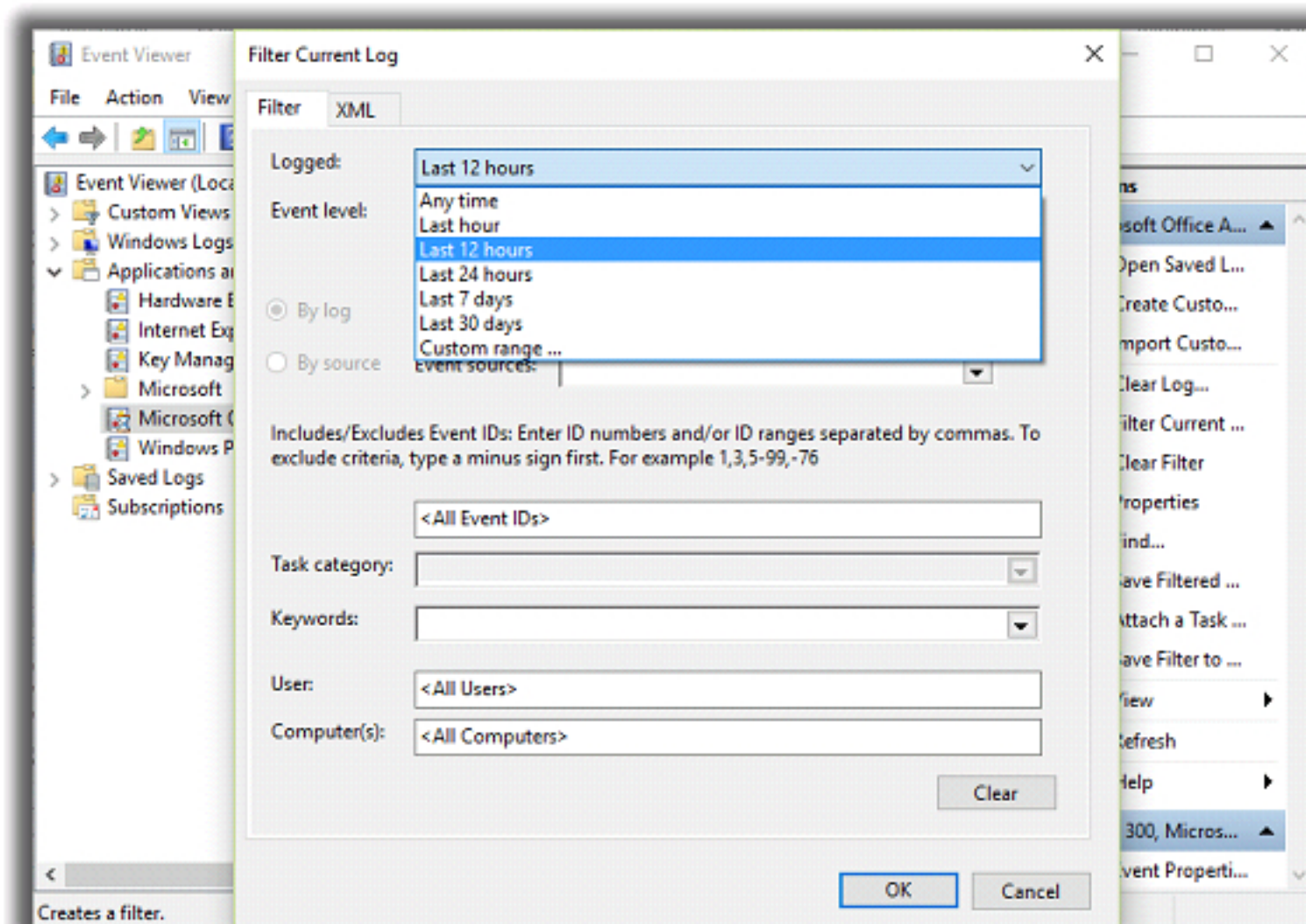





FIGURE 6.6: Event Viewer's filter window

Windows Event Log File Internals







The Windows Event Log files are, essentially, databases with the records related to the system, security, and applications




The databases related to the system are stored in a file named **System.evtx**



The databases related to security are stored in a file named **Security.evtx**



The databases related to applications are stored in a file named **Application.evtx**




Windows event logs are stored in: **C:\Windows\System32\winevt\Logs** folder

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

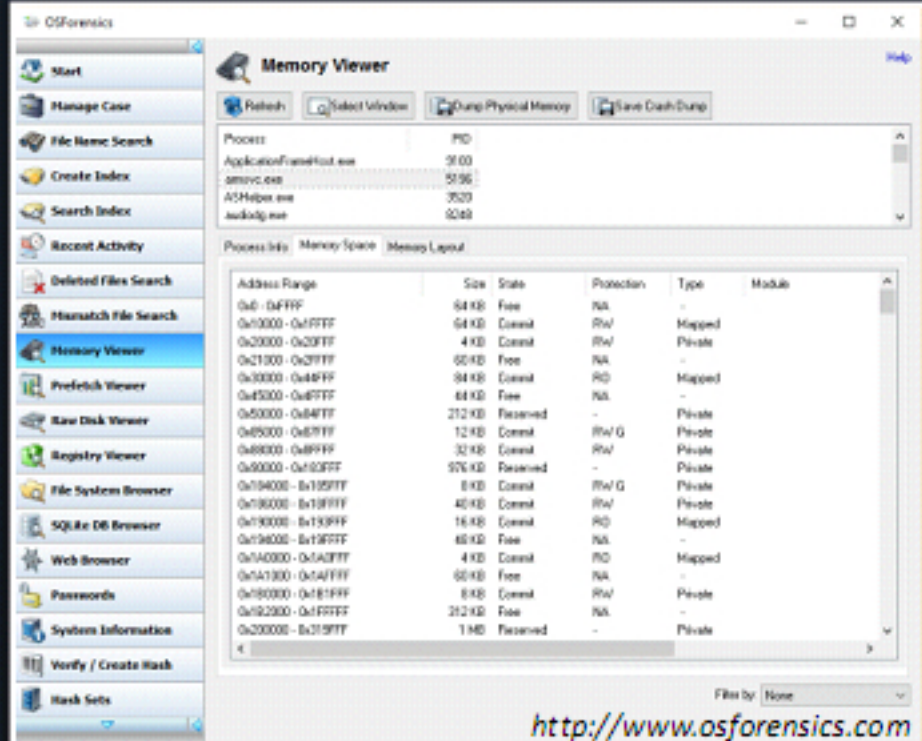
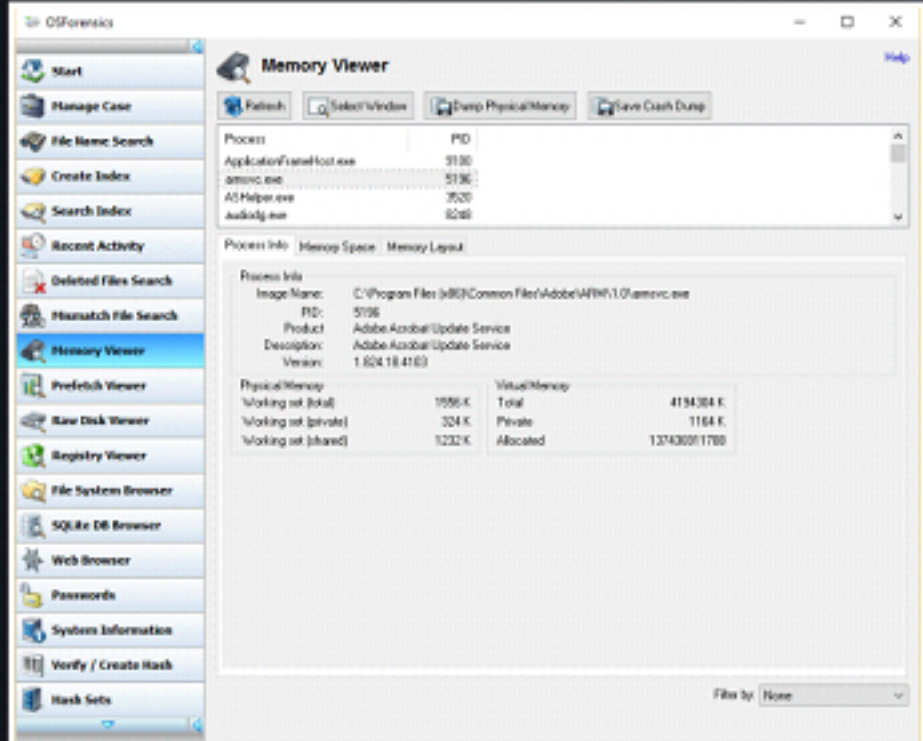
The Windows event log files contain the records related to the system, security, and applications stored in separate files named System.evtx, Security.evtx, and Application.evtx, respectively. They are stored in the **C:\Windows\System32\winevt\Logs** folder.

Each of the event log file databases is similarly constructed. Each file has a header, a floating footer of sorts, and records. Database slack exists in the logical portion of the file outside the proper database. To keep the files from becoming fragmented, the operating system may allocate large contiguous cluster runs to the event log files.

Windows Forensics Tools: OS Forensics



- OSForensics allows to identify suspicious files and activity with **hash matching, drive signature comparisons, e-mails, memory and binary data**
- It helps to extract forensic evidences from computers with advanced file searching and indexing and also enables this data to be managed effectively




Address Range	Size	State	Protection	Type	Module
0x0 - 0xFFFF	64 KB	Free	NA	-	-
0x10000 - 0x1FFFF	64 KB	Commit	R/W	Mapped	-
0x20000 - 0x2FFFF	4 KB	Commit	R/W	Private	-
0x30000 - 0x3FFFF	60 KB	Free	NA	-	-
0x40000 - 0x4FFFF	64 KB	Commit	RD	Mapped	-
0x50000 - 0x5FFFF	64 KB	Free	NA	-	-
0x60000 - 0x6FFFF	212 KB	Reserved	-	Private	-
0x70000 - 0x7FFFF	12 KB	Commit	R/W G	Private	-
0x80000 - 0x8FFFF	32 KB	Commit	R/W	Private	-
0x90000 - 0x9FFFF	976 KB	Reserved	-	Private	-
0xA0000 - 0xAFFFF	8 KB	Commit	R/W G	Private	-
0xB0000 - 0xBFFFF	40 KB	Commit	R/W	Private	-
0xC0000 - 0xCFFFF	16 KB	Commit	RD	Mapped	-
0xD0000 - 0xDFFFF	60 KB	Free	NA	-	-
0xE0000 - 0xEFFFF	4 KB	Commit	RD	Mapped	-
0xF0000 - 0xFFFF	60 KB	Free	NA	-	-
0x100000 - 0x10FFFF	8 KB	Commit	R/W	Private	-
0x110000 - 0x11FFFF	212 KB	Free	NA	-	-
0x120000 - 0x12FFFF	1 MB	Reserved	-	Private	-











<http://www.osforensics.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OS Forensics is a system information gathering software, which extracts forensic data from computers and uncovers everything hidden inside a PC. It identifies suspicious files and activities with hash matching; it also makes drive signature comparisons, and looks into emails, memory, and binary data. It analyzes the results in the form of a file listing, a thumbnail view, or a timeline view, which allows you to determine at what point some significant file change activity has occurred.

Windows Forensics Tools (Cont'd)



 Belkasoft Evidence Center http://belkasoft.com	 Proc Heap Viewer http://securityxploded.com
 RegScanner http://www.nirsoft.net	 Memory Viewer http://www.rjlsoftware.com
 MultiMon http://www.resplendence.com	 Word Extractor http://www.soft.tahionic.com
 Process Explorer https://technet.microsoft.com	 Belkasoft Browser Analyzer http://belkasoft.com
 Security Task Manager http://www.neuber.com	 Metadata Assistant http://www.thepaynegroup.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Belkasoft Evidence Center

Source: <http://belkasoft.com>

Belkasoft Evidence Center helps investigators to search, analyze, and store digital evidences found in Instant Messenger histories, Internet browser histories, and Outlook mailboxes.

Features:

- All major Instant Messengers (Windows and Mac OS), browsers, and email clients are supported.
- Image and video file analysis for pornography, faces, and text is available.
- Analyzed information is persistently stored in the database.
- Stored evidence is broken up by case.
- Deleted history retrieval is supported.
- Encase, SMART, and DD images can be mounted, including Windows and Mac OS drives.
- Live memory analysis is available, including hibernation and page files analysis.
- Huge cases (e.g., containing several 10-Gb mailboxes) are supported.
- Enterprise edition allows for simultaneous work of multiple users.

RegScanner

Source: <http://www.nirsoft.net>

RegScanner is a small utility that allows you to scan the registry, find the desired registry values that match the specified search criteria, and display them in one list. After finding the registry values, you can jump to the right value in RegEdit, by double-clicking the desired registry item. You can also export the found registry values into a .reg file that can be used in RegEdit.

Features:

- RegScanner utility displays the entire search result at once, so you don't have to press F3 in order to find the next value.
- In addition to the standard string search (like in RegEdit), RegScanner can find registry values by data length, value type (REG_SZ, REG_DWORD, and so on), and by modified date of the key.
- RegScanner can find a Unicode string located inside a binary value.
- RegScanner allows you to make a case-sensitive search.
- While scanning the registry, RegScanner can display the currently scanned registry key, as opposed to RegEdit, which simply displays a "Searching the registry" dialog box.

MultiMon

Source: <http://www.resplendence.com>

MultiMon is an advanced multifunctional system monitoring tool for Windows OS that displays highly detailed output of a very wide range of system activities in real time. The registry monitor shows registry activity in real time. It also allows you to monitor clipboard, keyboard, and task activities. It allows you to export output to text files and sort output views by column. All activities are recorded with lots of details, including a high-precision time stamp, process name and ID, thread ID, CPU ID, object handle, and window title.

Process Explorer

Source: <http://technet.microsoft.com>

Process Explorer shows the information about which handles and DLLs processes have been opened or loaded. The Process Explorer display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in: if it is in handle mode you'll see the handles that the process selected in the top window has opened; if Process Explorer is in DLL mode you'll see the DLLs and memory-mapped files that the process has loaded. Process Explorer also has a powerful search capability that will show you, which processes have particular opened handles or loaded DLLs.

Security Task Manager

Source: <http://www.neuber.com>

Security Task Manager shows comprehensible information about programs and processes running on the computer. The Windows Task Manager, provides:

- Unique security risk rating
- Free online scan with all known anti-virus engines
- Full directory path and file name
- Process description
- CPU usage graph
- Embedded hidden functions
- Process type

The Security Task Manager detects unknown malware and rootkits hidden from anti-virus software.

Proc Heap Viewer

Source: <http://securityxploded.com>

Proc Heap Viewer enumerates process heaps on Windows. It uses a much better technique than the Windows heap API functions, which makes it really fast and highly efficient. You can enumerate the heaps from normal Windows processes as well as system services. The Vulnerability researchers can use it as a side tool for discovering heap-related vulnerabilities. Proc Heap Viewer is a portable tool that comes with an installer for local installation and uninstallation of the software. It also presents an enhanced user interface.

Memory Viewer

Source: <http://www.rjlsoftware.com>

With Memory Viewer, you can view your system memory configuration. The Memory Viewer Not only does Memory Viewer show you the channel, dimm, size, and speed, it also shows you the type of memory: SDRAM, DDR, etc. Memory Viewer can save you time by telling you detailed information about the memory cards installed in your computer, as well as the current memory allocation.

With Memory Viewer, you can get information such as the physical location on the motherboard, channel, dimm number, device type, bank locator, synchronous type, dimm factor, chip size, memory speed, total width, manufacturer, serial number, asset tag, part number, and more. Memory Viewer retrieves the most information from your Windows system memory.

Word Extractor

Source: <http://www.soft.tahionic.com>

Word Extractor converts binary files (like Windows EXE applications, DLLs, and encrypted files) to text files, allowing you to look inside. The Word Extractor tool can be used with any file in your computer. You can use it to separate the strings that contain human text or words from binary code (like applications, DLLs). Virtually, it has an infinite number of uses. This makes it a much-desired tool not only for advanced users but also for beginners.

It is suitable for many purposes, such as:

- Finding cheats in games
- Finding hidden text in any files (EXE applications, binary, DLL)
- Finding hidden passwords in any files (EXE applications, binary, DLL)
- Recovering corrupted documents (like Microsoft Word, RTF)
- Converting binary files to text files
- Checking suspicious files (software) against viruses and malware

Belkasoft Browser Analyzer

Source: <http://home.belkasoft.com>


Belkasoft Browser Analyzer allows you to search and analyze various Internet browser histories. It supports all popular browsers. It can retrieve URLs, passwords, and cookies. The user does not have to be logged on as the history owner. No write access to a drive is required. Cached sites can be visualized and exported to text, HTML, and XML formats.











Metadata Assistant

Source: <http://www.payneconsulting.com>

The Metadata Assistant analyzes Word/Excel/PowerPoint (2000 and higher) files to determine the type and amount of metadata (hidden information) that exists within. You can use a variety of options to remove unwanted metadata from your documents, workbooks, and presentations. You can analyze and clean the active (open) file in any of those applications or you can designate a specific closed file. You can even use the Metadata Assistant to batch process multiple files located on a local or network folder. Additionally, you can analyze and clean files attached to outbound email messages and convert them to PDF format for extra protection.

Windows Forensics Tools (Cont'd)



 HstEx http://www.digital-detective.net	 ProDiscover Forensic http://www.arcgroupny.com
 XpoLog Log Management http://xpolog.com	 Helix3 Pro http://www.e-fense.com
 Event Log Explorer http://eventlogxp.com	 ThumbsDisplay http://www.infinadyne.com
 LogMeister http://www.logmeister.com	 Registry Viewer http://accessdata.com
 System Explorer http://systemexplorer.net	 Windows Forensic Toolchest (WFT) http://www.foolmoon.net

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

HstEx

Source: <http://www.digital-detective.co.uk>

HstEx is a Windows-based, advanced professional forensic data recovery solution designed to recover browser artifacts and Internet history from a number of different source evidence types. HstEx supports all of the major forensic image formats.

It finds deleted Internet history from:

- Unallocated clusters
- Cluster slack
- Live memory, memory dumps, and crash dumps
- Page files, system files, and hibernation files
- System restore points

XpoLog Log Management

Source: <http://xpolog.com>

XpoLog turns your Data into actionable insights, with in-depth analytics. From the XpoLog Log Viewer, you can investigate single logs, filter out specific strings, and dig in deep. You can open multiple log viewer tabs, to compare intimate details of different logs. XpoLog Search allows

you to search and view multiple logs and file sources. XpoLog displays your search results and displays each event automatically with an auto-detected severity level.

Features:

- Collects live log data over SSH connection with very high throughput
- Receives log events via common protocols like SysLog and HTTP
- Collect any log file format (txt, json, xml...) across dynamic cyclic files archived such as Zip, Gzip, binary formats
- Has the architecture to maintain a high availability grid that supports data collection of files, events, databases

Event Log Explorer

Source: <http://www.eventlogxp.com>

Event Log Explorer is a software solution for viewing, monitoring, and analyzing events recorded in security, system, application, and other logs of Microsoft Windows operating systems. It helps to quickly browse, find, and report on problems, security warnings, and all other events that are generated within Windows.

Features:

- Use a multiple-document or tabbed-document interface, depending on user preferences.
- Favorite computers and their logs are grouped into a tree.
- Back up event logs manually and automatically.
- Event descriptions and binary data are in the log window
- Advanced filtering is possible by any criteria, including event description text
- The Quick Filter feature allows you to filter event log in a couple of mouse clicks
- Log loading options to pre-filter event logs
- Use bookmarks for fast navigation between events
- It is compatible with well-known event knowledge-bases (EventID.com and Microsoft knowledgebase)
- Color coding by event ID is possible
- Print and export logs to different formats
- Read damaged EVT files and generate EVT files from event views

LogMeister

Source: <http://www.logmeister.com>

LogMeister monitors virtually any log your systems and applications can generate, including event logs, text logs and RSS. It will alert you to critical events throughout your network,

facilitate central archiving of log data, and assist with analysis and meeting audit requirements. As LogMeister is a centralized monitoring solution, there is no need to install agents on monitored PC's and servers.

Features:

Monitor any log on your network (Windows security & other event logs, syslog and any text log, including Unix)

- Choose from real-time or scheduled monitoring on a per-log basis
- Aggregate event log data
- Configurable real-time filters, alerts & actions
- Syslog forwarding for any log type
- Flexible archiving, data export and reporting options
- Agentless solution with limitless scalability

System Explorer

Source: <http://systemexplorer.net>

System Explorer is free software for exploration and management of system internals. This software includes tools to help you keep your system under control. It gives detailed information about tasks, processes, modules, startups, IE add-ons, uninstallers, Windows, services, drivers, connections, and opened files.

Features:

- Easy check of suspicious files via VirusTotal, Jotti service, or our File Database
- Easy monitoring of processes, activities, and system changes
- Usage graphs of important system resources
- Tray icon with detailed system and battery status
- WMI browser and additional system info
- Multilanguage support

ProDiscover Forensics

Source: <http://www.techpathways.com>

ProDiscover Forensics is a computer security tool that enables computer professionals to find all the data on a computer disk while protecting evidence and creating evidentiary quality reports for use in legal proceedings.

Features:

- Creates bit-stream copy of disk
- Searches files or entire disk including slack space, HPA section

- Previews all files, even if hidden or deleted, without altering data on disk
- Maintains multi-tool compatibility by reading and writing images in the pervasive UNIX dd format and reading images in E01 format
- Automatically generates and records MD5, SHA1, or SHA256 hashes to prove data integrity

Helix3 Pro

Source: <http://www.e-fense.com>

Helix3 Pro is the cyber security solution providing incident response, computer forensics and e-discovery.

Features:

- A multi-platform LIVE side for three environments; Mac OS X, Windows and Linux
- A bootable forensically sound environment to boot x86 system

ThumbsDisplay

Source: <http://www.infinadyne.com>

ThumbsDisplay is a tool for examining and reporting on the contents of Thumbs.db files used by Windows. The tool prints a full-page version of thumbnail images without any other graphics programs. It will copy individual thumbnails and print three different format reports.

Features:

- Show all thumbnail files: thumbs.db, thumbcache_idx.db, thumbcache_32.db, thumbcache_96.db, thumbcache_256.db, thumbcache_1024.db, and thumbcache_sr.db. Find them in all locations quickly using the built-in locator.
- Display all thumbnail images with original file name and timestamp.
- Use the built-in locator for all thumbnail files. It performs a high-speed search for these files, which are normally hidden from Windows users. From the locator, you can then open any file shown and display the full content.
- Prints individual images as a full page or select from the three report formats: Report, Contact Sheet, and All items.
- Copies individual images to the clipboard for inclusion in a document, or save them as JPEG or BMP format files.
- Displays thumbnails in three sizes: 96x96 (original) 150x150, or 200x200.

Registry Viewer

Source: <http://accessdata.com>

Registry Viewer allows you to view the contents of Windows operating system registries. Unlike the Windows Registry Editor, which displays only the current system's registry, Registry Viewer lets you view registry files from any Windows system. Registry Viewer also provides access to a

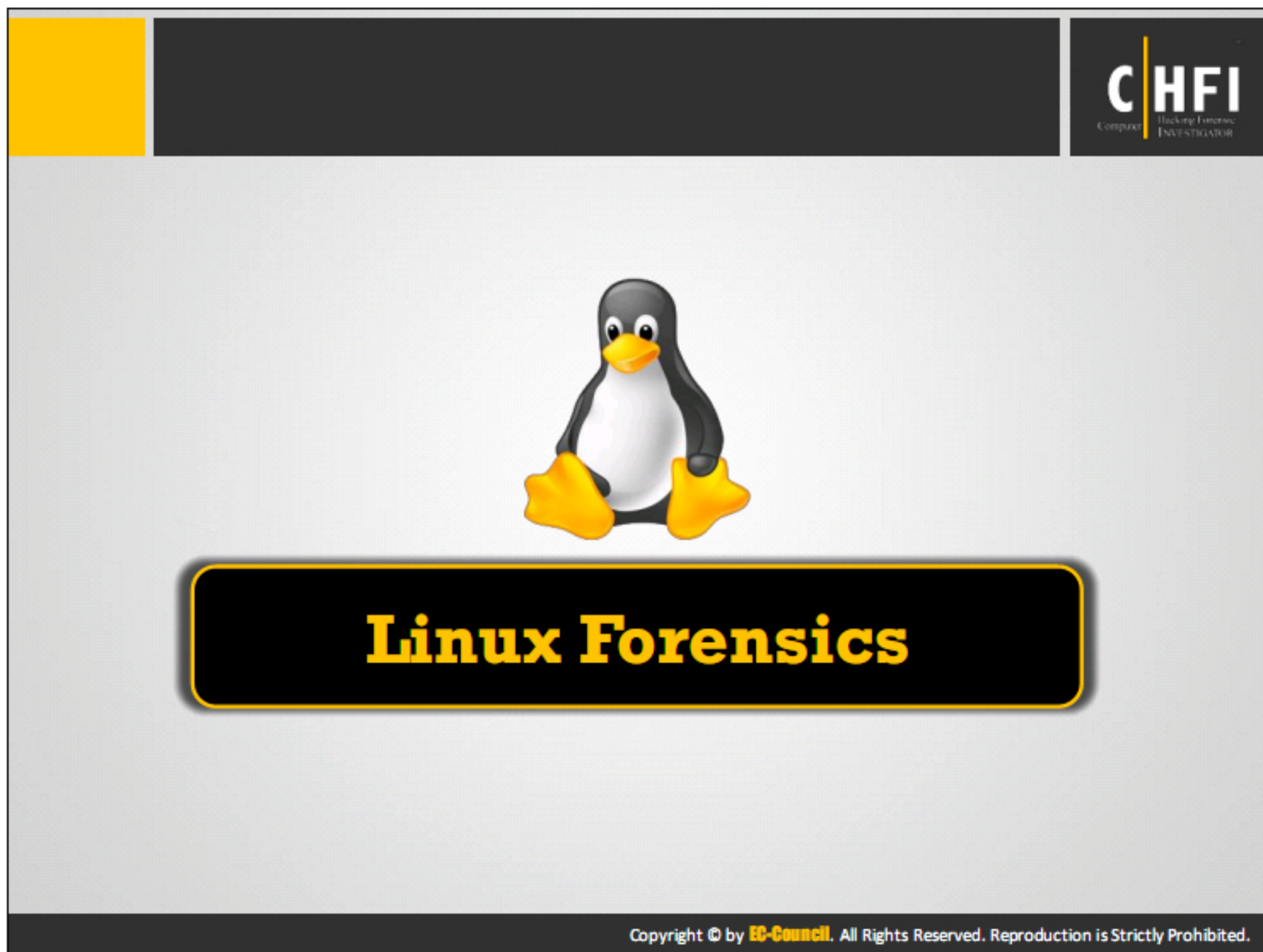
registry's encrypted protected storage, which contains passwords, usernames, and other information not accessible in Windows Registry Editor.

The Registry Viewer provides access to the encrypted "Protected Storage System Provider" key, which potentially contains data from Internet data entries, Microsoft Outlook and Outlook Express passwords, website logon stored passwords, and search queries from Google, Yahoo, and potentially more. The Windows registry is a set of data files that allows the Windows operating system to control hardware, software, user information, and the overall functionality of the Windows interface.

Windows Forensic Toolchest (WFT)


Source: <http://www.foolmoon.net>


The Windows Forensic Toolchest (WFT) is designed to provide a structured and repeatable automated live forensic response, incident response, or audit on a Windows system while collecting security-relevant information from the system. WFT is essentially a forensically enhanced batch processing shell, capable of running other security tools and producing HTML-based reports in a forensically sound manner.



Linux forensics refers to performing forensic investigation on a Linux operated device. To do so, the investigators should have a good understanding on the techniques required to conduct live analysis; to collect volatile and non-volatile data, along with knowledge of various shell commands and the information they can retrieve. The investigators should also be aware of the Linux log files, their storage and location in the directory, as they are the most important sources of information to trace down the attacker. This module will walk you through the various shell commands, methods to collect volatile data, the different log files and the information they provide.

Shell Commands



Investigators can use Linux commands to gather necessary information from the system 

Some of the useful commands include:

dmesg

Displays kernel ring buffers or information about device drivers loaded into the kernel

Syntax: `dmesg | grep -i eth0` (Displays hardware information of the Ethernet port eth0)

fsck

Stands for file system consistency check and helps to check and repair any file system

Syntax: `fsck -A` (Checks all configured filesystems)

stat

Displays file or file system status

Syntax: `stat [OPTION]... FILE...`

history

Lists the Bash's log of the typed commands

Syntax: `history n` (Lists the last n commands)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigators use the shell commands in Linux for collecting information from the system. Some of the frequently used commands include:

dmesg

The command **dmesg** is the short for display message or 'Driver Message'. The command displays the kernel ring buffers, which contains the information about the drivers loaded into kernel during boot process and error messages produced at the time of loading the drivers into kernel. These messages are helpful in resolving the restoring the device's driver issues.

Syntax: dmesg options

`dmesg | grep -i eth0` (Displays hardware information of the Ethernet port eth0)

fsck

The command **fsck**, is meant for File System Consistency Check. It is a tool to check the consistency of Linux file system and repair.

Syntax: `fsck -A` (Checks all configured filesystems)

Stat

Displays file or file system status.

Syntax: `stat [OPTION]... FILE...`

history

The command **history** checks and lists the Bash shell commands used. This command helps the users for auditing purposes.

Syntax: **history n** (Lists the last n commands)

mount

The command **mount** causes mounting of a file system or a device to the directory structure, making it accessible by the system.

Syntax: **mount -t type device dir** (Requests kernel to attach the file system found on device of type type at the directory dir)

Shell Commands (Cont'd)



mount

Mounts a file system

Syntax: `mount -t type device dir` (Requests kernel to attach the file system found on device of type type at the directory dir)

ps

Used to report the status of current process

Syntax: `ps -ef` (Displays information about all the processes in the system)

ps tree

Displays the processes on a system in the form of a tree

Syntax: `ps tree -h` (Highlights the current process and its ancestors)

grep

Searches for presence of text or an expression or pattern in files

Syntax: `grep -i jpg filelist.list` (Looks for the pattern "jpg" in the list of files)

top

Displays system summary information as well as a list of processes or threads Linux kernel is currently managing

Syntax: `top -hv` (Displays the library version and the usage prompt)


kill

Terminates the processes without logging out or rebooting the system

Syntax: `kill -9 0710` (Terminates the process with ID 0710 using the kill signal)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Shell Commands (Cont'd)



file

Displays the type of data contained in a computer file

Syntax: `file *` (Displays information about all the files present in the current dictionary)

su

Allows user to run a command with substitute user and group ID

Syntax: `su root` (Ownership of the session is changed to root and needs password)

dd

Copies a file, converts and formats it according to the operands

Syntax: `dd [operand]`

ls

Lists directory contents

Syntax: `ls -R` (list recursively directory tree)

pgrep

Stands for "Process-ID Global Regular Expressions Print", searches through the current processes and lists the process IDs which match the selection criteria to stdout

Syntax: `pgrep -u root sshd` (Lists the processes called sshd and owned by root)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Linux Log Files		CHFI Computer Hacking Forensic Investigator	
Log Location	Content Description		
/var/log/auth.log	System authorization information, including user logins and authentication mechanism		
/var/log/kern.log	Initialization of kernels, kernel errors or informational messages sent from kernel		
/var/log/faillog	Failed user login attempts		
/var/log/lpr.log	Stores printer logs		
/var/log/mail.*	All mail server message logs		
/var/log/mysql.*	MySQL server logs		
/var/log/apache2/*	Apache web server logs		
/var/log/apport.log	Application crash report / log		
/var/log/lighttpd/*	Lighttpd web server log files directory		
/var/log/daemon.log	Running services such as squid, ntpd, etc.		
/var/log/debug	Debugging log messages		
/var/log/dpkg.log	Package installation or removal logs		

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Log files are records of all the activities performed over an operating system. Linux log files store information about the system's kernel and the services running in the system. In Linux OS, different log files hold different information, which helps the investigators to analyze various issues during a security incident.

Investigators should learn and understand about the contents of various log files, which will help them during security incidents and help them understand the locations they might have to look for finding potential evidences.

Below mentioned are some locations for Linux log files, which can help the investigators to find out the required data and resolve the issues. Additional log locations include:

/var/log/messages	Global system messages
/var/log/dmesg	Kernel ring buffer information
/var/log/cron	Information about the cron job in this file
/var/log/user.log	All user level logs
/var/log/lastlog	Recent login information
/var/log/boot.log	Information logged on system boots

TABLE 06.5: Log locations in Linux

Collecting Volatile Data

CHFI
Computer Hacking Forensic Investigator

- Run the **netstat** command to extract network information
- It displays network connections, routing tables, and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics

- Run **last -F** command to see the users' full login and logout times and dates of the system



```
root@kali:~# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State           I-Node  Path
unix 2      [ ]     DGRAM     0
unix 3      [ ]     DGRAM     0
unix 17     [ ]     DGRAM     0
unix 7      [ ]     DGRAM     0
unix 2      [ ]     DGRAM     0
unix 2      [ ]     DGRAM     0
unix 3      [ ]     STREAM    CONNECTED      20573
unix 3      [ ]     STREAM    CONNECTED      19384
unix 3      [ ]     STREAM    CONNECTED      13532
unix 3      [ ]     STREAM    CONNECTED      96916
unix 3      [ ]     STREAM    CONNECTED      20622
unix 3      [ ]     STREAM    CONNECTED      19275
unix 3      [ ]     STREAM    CONNECTED      16344
unix 3      [ ]     STREAM    CONNECTED      16241
unix 3      [ ]     STREAM    CONNECTED      20564
unix 3      [ ]     STREAM    CONNECTED      20540
unix 3      [ ]     STREAM    CONNECTED      18759
unix 3      [ ]     DGRAM     0
unix 3      [ ]     STREAM    CONNECTED      13388
unix 3      [ ]     STREAM    CONNECTED      20895
unix 3      [ ]     STREAM    CONNECTED      19744
```

```
root@kali:~# last -F
root        tty2      :1                Wed Jun  8 09:10:21 2016   still logged in
reboot     system boot  4.9.0-kali1-amd64 Wed Jun  8 13:39:21 2016   still running
lode       tty3      :2                Thu Jun  2 03:25:37 2016   - crash                (6-10-13)
lason      tty3      :2                Thu Jun  2 03:24:54 2016   - Thu Jun  2 03:25:12 2016 (60:00)
martin     tty3      :2                Thu Jun  2 03:24:17 2016   - Thu Jun  2 03:24:38 2016 (60:00)
root       tty2      :1                Thu Jun  2 03:23:38 2016   - crash                (6-10-15)
reboot     system boot  4.9.0-kali1-amd64 Wed Jun  1 17:29:39 2016   still running
wtmp begins Thu Jun  2 03:22:13 2016
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Volatile Data (Cont'd)

CHFI
Computer Hacking Forensic Investigator

Run **hostname** command to see the system hostname

Run **ifconfig -a** command to view the configuration of all network interfaces on the system

```
root@kali:~# hostname
kali
root@kali:~#
```

```
root@kali:~# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.0.7 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::215:5dff:fe00:11b prefixlen 64 scopeid 0x20<link>
    ether 08:15:5d:00:01:1b txqueuelen 1000 (Ethernet)
    RX packets 7828 bytes 1103707 (1.1 MiB)
    RX errors 0 dropped 1 overrun 0 frame 0
    TX packets 28 bytes 1969 (1.9 KiB)
    TX errors 0 dropped 0 overrun 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 19.0.0.11 netmask 255.0.0.0 broadcast 19.255.255.255
    inet6 fe80::215:5dff:fe00:121 prefixlen 64 scopeid 0x20<link>
    ether 08:15:5d:00:01:21 txqueuelen 1000 (Ethernet)
    RX packets 114 bytes 8211 (8.0 KiB)
    RX errors 0 dropped 0 overrun 0 frame 0
    TX packets 16 bytes 1192 (1.1 KiB)
    TX errors 0 dropped 0 overrun 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 0 (Local Loopback)
    RX packets 72 bytes 4320 (4.2 KiB)
    RX errors 0 dropped 0 overrun 0 frame 0
    TX packets 72 bytes 4320 (4.2 KiB)
    TX errors 0 dropped 0 overrun 0 carrier 0 collisions 0
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Volatile Data (Cont'd)



Run **lsof** (list open files) command to list all open files and the active processes that opened them

Run **lsmod** command that displays loaded modules

```
root@kali:~# lsof
ls: cannot stat('lsof'): file system /run/user/1000/gvfs
Output information may be incomplete.
COMMAND PID TID USER FD TYPE DEVICE SIZE/OFF NODE NAME
systemd 1 1 root cwd DIR 8,1 4096 2 /
systemd 1 1 root rtd DIR 8,1 4096 2 /
systemd 1 1 root txt REG 8,1 1536160 165816 /lib/systemd/systemd
libaudit.so.1.2.0 1 1 root exe REG 8,1 18824 117836 /lib/x86_64-linux-gnu
systemd 1 1 root exe REG 8,1 266794 117833 /lib/x86_64-linux-gnu
libnlsid.so.1.1.0 1 1 root exe REG 8,1 18640 117859 /lib/x86_64-linux-gnu
libattr.so.1.1.0 1 1 root exe REG 8,1 14640 117832 /lib/x86_64-linux-gnu
systemd 1 1 root exe REG 8,1 456032 117852 /lib/x86_64-linux-gnu
libc-2.21.so 1 1 root exe REG 8,1 1710188 117871 /lib/x86_64-linux-gnu
libpthread-2.21.so 1 1 root exe REG 8,1 133576 117869 /lib/x86_64-linux-gnu
libcrypt.so.2.1.2 1 1 root exe REG 8,1 292320 117840 /lib/x86_64-linux-gnu
libmount.so.1.1.0 1 1 root exe REG 8,1 68880 117855 /lib/x86_64-linux-gnu
libapparmor.so.1.3.0
```

```
root@kali:~# lsmod
Module Size Used by
bnep 20480 2
fuse 94208 0
nfnetlink_queue 20480 0
nfnetlink_log 20480 0
nfnetlink 16384 2 nfnetlink_log,nfnetlink_queue
bluetooth 512000 5 bnep
rfkill 24576 4 bluetooth
binfmt_misc 20480 1
loef_ansi 16384 0
scsi_kr 16384 0
scsiouse 122976 0
serio_raw 16384 0
sg 32768 0
hyperkey_keyboard 16384 0
nv_ufix 24576 0
p250_firmware 16384 0
hyperkey_fd 20480 0
acpi_cpufreq 20480 0
button 16384 0
processor 36864 1 acpi_cpufreq
acpi 20480 12
l2c_pl110 24576 0
lovedev 20480 0
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Volatile Data (Cont'd)



- Xclip is a command line interface to the X clipboard
- Run **xclip -o** to output the contents of the clipboard

- Run **aureport** command to see the summary report of audit daemon logs

```
root@kali:~# cat .bash_history | xclip
root@kali:~# xclip -o
ifconfig
ifconfig eth0 192.168.0.24
ifconfig
service apache2 status
service apache2 start
service apache2 start
leafpad /etc/network/interfaces
ifdown eth1
ifup eth1
ifconfig
netstat
hostname
clear
hostname
clear
lsof
clear
lsof
lsmod
aureport
msfconsole
```

```
root@kali:~# aureport
Summary Report
=====
Range of time in logs: 06/01/2016 08:37:17.203 - 06/01/2016 08:37:17.203
Selected time for report: 06/01/2016 08:37:17 - 06/01/2016 08:37:17.203
Number of changes in configuration: 0
Number of logins to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 0
Number of failed authentications: 0
Number of users: 1
Number of terminals: 0
Number of host names: 0
Number of executables: 0
Number of commands: 0
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Volatile Data (Cont'd)



- Run **id** command to determine the user ID for the specified username
- After that, run the **ausearch** command to track all the user events pertaining to that user ID

- Executable and Linking Format (ELF) is the main executable file format
- System stores **shared libraries**, **kernel modules**, and the **kernel** in ELF Format
- Run **readelf** command to analyze the headers and sections of ELF files

```
root@kali:~# id root
uid=0(root) gid=0(root) groups=0(root)
root@kali:~# ausearch -ui 0 --interpre
type=USER_ACCT msg=audit(06/01/2016 08:39:01.414:1) : pid=48013 uid=root auid=unset ses=unset exe="/usr/sbin/cron hostname=? addr=? terminal=cron res=success"
type=CRED_ACQ msg=audit(06/01/2016 08:39:01.414:4) : pid=48013 uid=root auid=unset ses=unset exe="/usr/sbin/cron hostname=? addr=? terminal=cron res=success"
type=LOGIN msg=audit(06/01/2016 08:39:01.414:5) : pid=48013 uid=root old-auid=unset auid=root old-ses=4204967295 ses=70 res=yes
type=USER_START msg=audit(06/01/2016 08:39:02.794:6) : pid=48013 uid=root auid=root ses=70 exe="/usr/sbin/cron hostname=? addr=? terminal=cron res=success"
type=CRED_DISP msg=audit(06/01/2016 08:39:02.794:7) : pid=48013 uid=root auid=root ses=70 exe="/usr/sbin/cron hostname=? addr=? terminal=cron res=success"
type=USER_END msg=audit(06/01/2016 08:39:02.794:8) : pid=48013 uid=root auid=root ses=70 exe="/usr/sbin/cron hostname=? addr=? terminal=cron res=success"
type=SERVICE_START msg=audit(06/01/2016 08:45:13.386:9) : pid=1 uid=root auid=unset ses=unset exe="/usr/sbin/cron hostname=? addr=? terminal=? res=success"
type=SERVICE_STOP msg=audit(06/01/2016 08:45:43.539:10) : pid=1 uid=root auid=unset ses=unset exe="/usr/sbin/cron hostname=? addr=? terminal=? res=success"
type=SERVICE_START msg=audit(06/01/2016 08:46:28.414:11) : pid=1 uid=root auid=unset ses=unset exe="/usr/sbin/cron hostname=? addr=? terminal=? res=success"
```

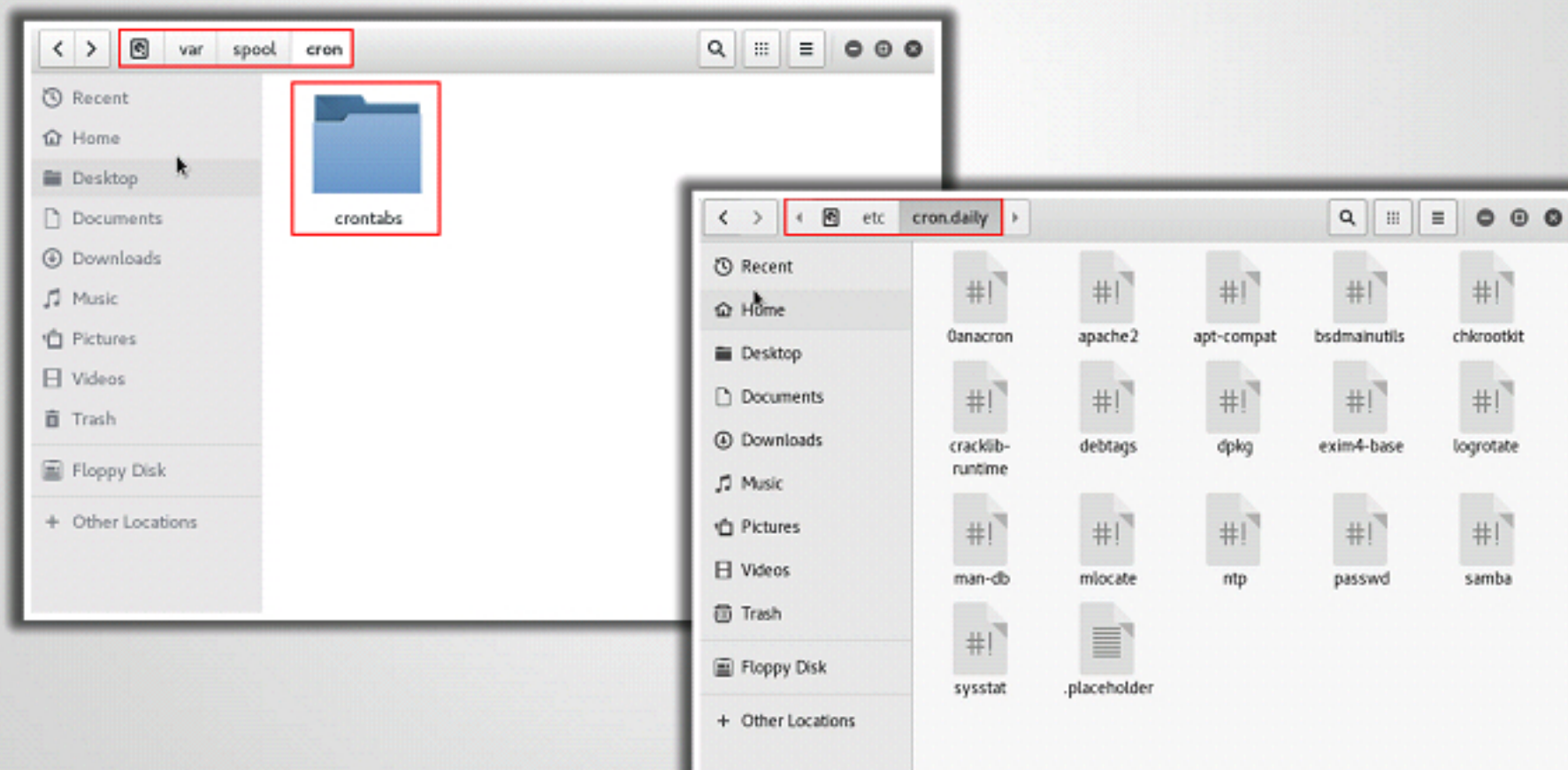
```
root@kali:~# readelf -h /sbin/showmount
ELF Header:
  Magic: 7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00
  Class: ELF64
  Data: 2's complement, little endian
  Version: 1 (current)
  OS/ABI: UNIX - System V
  ABI Version: 0
  Type: EXEC (Executable file)
  Machine: Advanced Micro Devices X86-64
  Version: 0x1
  Entry point address: 0x401969
  Start of program headers: 64 (bytes into file)
  Start of section headers: 15192 (bytes into file)
  Flags: 0x0
  Size of this header: 64 (bytes)
  Size of program headers: 56 (bytes)
  Number of program headers: 8
  Size of section headers: 64 (bytes)
  Number of section headers: 27
  Section header string table index: 26
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Volatile Data (Cont'd)




- Verify the contents of **/var/spool/cron/** and **/etc/cron.daily** to collect information about any scheduled tasks



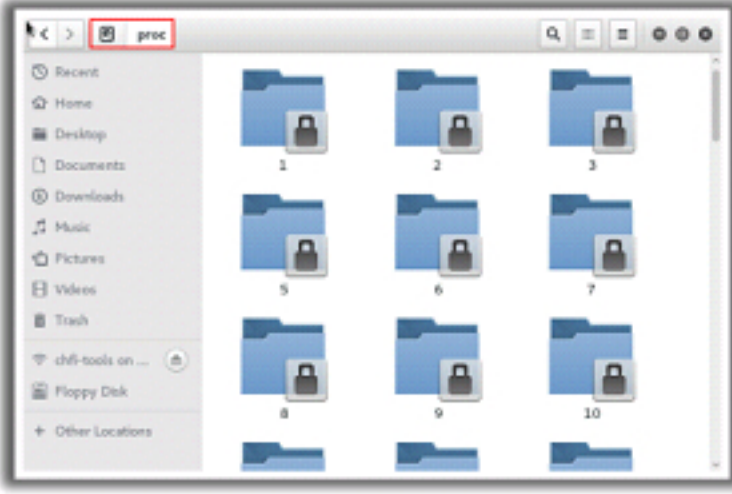

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Volatile Data (Cont'd)



Acquire the command history from the **.bash_history** file

Collect the current state data of a Linux system from the **/proc** directory



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

.bash_history

The **.bash_history** file stores the command history. These file helps the investigator to analyze the commands used in the terminal by the malicious user.

/proc

The **/proc/** directory is also known as **proc** file system. The directory comprises of the order of special files that represent the current state of a kernel. Investigators can find the information of the systems hardware and the processes running them. The **proc** file system acts as interface for the internal data structures within the kernel.

Collecting Volatile Data (Cont'd)

**1**

Run **ps** command to view the processes running on the system

2

It provides a **snapshot** of the **current processes** along with detailed information like **user id**, **CPU usage**, **memory usage**, **command name**, etc.

3

Check the **process tree** to determine any suspicious **child processes** and **dependencies**

```
root@kali: ~# ps auxww
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3 121284 4516 ?        Ss   May31   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S    May31   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    May31   0:01 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   May31   0:00 [kworker/0:0H]
root         6  0.0  0.0      0     0 ?        S    May31   0:00 [kworker/u128:0]
root         7  0.0  0.0      0     0 ?        S    May31   0:00 [rcu_sched]
root         8  0.0  0.0      0     0 ?        S    May31   0:00 [rcu_bh]
root         9  0.0  0.0      0     0 ?        S    May31   0:00 [migration/0]
root        10  0.0  0.0      0     0 ?        S    May31   0:00 [watchdog/0]
root        11  0.0  0.0      0     0 ?        S    May31   0:00 [kdevtmpfs]
root        12  0.0  0.0      0     0 ?        S<   May31   0:00 [netns]
root        13  0.0  0.0      0     0 ?        S<   May31   0:00 [perf]
root        14  0.0  0.0      0     0 ?        S    May31   0:00 [khungtaskd]
root        15  0.0  0.0      0     0 ?        S<   May31   0:00 [writeback]
root        16  0.0  0.0      0     0 ?        SN   May31   0:00 [kswapd]
root        18  0.0  0.0      0     0 ?        SN   May31   0:00 [kswapd0]
root        19  0.0  0.0      0     0 ?        S<   May31   0:00 [cryptod]
root        20  0.0  0.0      0     0 ?        S<   May31   0:00 [kintegrityd]
root        21  0.0  0.0      0     0 ?        S<   May31   0:00 [bioset]
root        22  0.0  0.0      0     0 ?        S<   May31   0:00 [kblockd]
root        23  0.0  0.0      0     0 ?        S<   May31   0:00 [devfreq_wq]
root        24  0.0  0.0      0     0 ?        S    May31   0:00 [kswapd0]
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ps

The command **ps** is the short notation for “process status”. The command is used to view the list of processes running in the system. It provides a snapshot of the current processes along with detailed information of user id, CPU usage, memory usage, command name, etc. Investigators can check for the tree to determine any suspicious processes and dependencies.

Collecting Volatile Data (Cont'd)



Run **arp** command to extract the ARP cache

```
root@kali:~# arp
Address          Hwtype Hwaddress      Flags Mask       Iface
192.168.0.123    ether  00:15:5d:00:b4:02 C          *    eth0
192.168.0.244    ether  d4:be:d9:c7:30:e6 C          *    eth0
gateway         ether  f4:0f:1b:1e:02:c1 C          *    eth0
192.168.0.182    (incomplete)
192.168.0.0      ether  00:15:5d:00:49:01 C          *    eth0
192.168.0.177    ether  74:86:7a:30:c2:44 C          *    eth0
192.168.0.140    ether  74:86:7a:23:96:40 C          *    eth0
192.168.0.157    ether  d4:be:d9:c3:c4:44 C          *    eth0
192.168.0.170    ether  78:45:c4:ac:64:5e C          *    eth0
192.168.0.24     ether  48:e2:44:c0:2e:19 C          *    eth0
192.168.0.156    ether  84:4b:f5:0e:a0:fb C          *    eth0
192.168.0.241    ether  24:b6:fd:57:c9:ab C          *    eth0
192.168.0.100    ether  24:b6:fd:40:e2:13 C          *    eth0
192.168.0.137    ether  a4:ba:db:fd:06:63 C          *    eth0
192.168.0.124    ether  d4:be:d9:c3:c7:a7 C          *    eth0
192.168.0.165    ether  ec:f4:bb:87:5a:d8 C          *    eth0
192.168.0.75     ether  14:36:c6:a3:0a:49 C          *    eth0
192.168.0.151    ether  00:25:11:22:2d:5f C          *    eth0
192.168.0.136    ether  48:5a:b6:23:3e:c1 C          *    eth0
```

Run **ss -l -p -n | grep <PID>** command to see if a particular process running on the system is suspicious

```
root@kali:~# ss -l -p -n | grep 1073
st    UNCONN    0      0      15:1073
st    UNCONN    0      0      15:1073
*str LISTEN  0      128    0/*tcp/*X11-unix/*X1 17996  * 0      users:
([*korg*.pid=1073,fd=4])
*str LISTEN  0      128    0/*tcp/*X11-unix/*X1 17997  * 0      users:
([*korg*.pid=1073,fd=6])
*str UNCONN  0      0      * 17987  * 0      users:([*korg*.pid=
1073,fd=1])
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Volatile Data (Cont'd)



Other commands to gather useful information about the compromised system:

- Run **cat /proc/version** command to know Linux kernel version used in the OS
- Run **cat /proc/sys/kernel/domainname** command to know the domain name
- Run **cat /proc/swaps** command to see total and used swap size
- Run **cat /proc/partitions** command to see the list of disk partitions

```
root@kali:~# cat /proc/version
Linux version 4.4.0-kali1-and64 (debian-kernel@lists.debian.org) (gcc version 5.3.1
20160307 (Debian 5.3.1-11) ) #1 SMP Debian 4.4.6-1kali1 (2016-03-18)
root@kali:~#
```

```
root@kali:~# cat /proc/sys/kernel/domainname
(none)
root@kali:~#
```

```
root@kali:~# cat /proc/swaps
Filename                                Type              Size      Used      Priority
/dav/sda5                              partition         1324020  0          -1
root@kali:~#
```

```
root@kali:~# cat /proc/partitions
major minor #blocks name
2        0          4 fd0
0        0    31457280 sda
0        1    30130176 sda1
0        2          1 sda2
0        5    1324032 sda5
11       0    1048575 wro
root@kali:~#
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Volatile Data (Cont'd)



- Run `cat /proc/cpuinfo` command to see details about the CPU on a machine

```
root@kali:~# cat /proc/cpuinfo
processor       : 0
vendor_id     : GenuineIntel
cpu family    : 6
model         : 59
model name    : Intel(R) Core(TM) i5-4260U CPU @ 1.60GHz
stepping      : 1
microcode    : 0x1d
cpu MHz       : 2381.000
cache size    : 3672 KB
physical id   : 0
siblings      : 1
core id       : 0
cpu cores     : 1
apicid        : 0
initial apicid: 0
fpu           : yes
fpu_exception: yes
cpuid level   : 13
wp            : yes
flags         : fpu vme de pse tsc mtr pae mce cx8 apic sep mtrr pge eca cco
pat pse36 clflush dts mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon pebs bts nopl xtopology tsc_reliable nonstop_tsc aperfperf
arfpnd pclmulqdq sse4_3 fma cx16 pcid sse4_2 x2apic movbe popcnt aes xsave
xsavecvt avx f16c rdrand hypervisor lahf_lm ida arat epb pln pts dtherm fsgsbase
bugs          :
bogomips      : 4682.00
clflush size  : 64
cache alignment: 64
address sizes : 48 bits physical, 48 bits virtual
power management:
```

- Run `cat /proc/self/mounts` to view the count points and mounted external devices

```
root@kali:~# cat /proc/self/mounts
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
devpts /dev/pts devpts rw,nosuid,relatime,size=1008672k,nr_inodes=252156,mode=755 0 0
devpts /dev/pts devpts rw,nosuid,nodev,noexec,relatime,gid=5,mode=620,pts=mode=000 0 0
tmpfs /run tmpfs rw,nosuid,nodev,relatime,size=204448k,mode=755 0 0
/dev/sda1 / ext4 rw,relatime,errors=remount-ro,data=ordered 0 0
securityfs /sys/kernel/security securityfs rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev/shm tmpfs rw,nosuid,nodev 0 0
tmpfs /run/lock tmpfs rw,nosuid,nodev,noexec,relatime,size=5120k 0 0
tmpfs /sys/fs/cgroup tmpfs ro,nosuid,nodev,noexec,mode=755 0 0
cgroup /sys/fs/cgroup/systemd cgroup rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/lib/systemd/systemd-cgroups-agent,name=systemd 0 0
pstore /sys/fs/pstore pstore rw,nosuid,nodev,noexec,relatime 0 0
cgroup /sys/fs/cgroup/freezer cgroup rw,nosuid,nodev,noexec,relatime,freezer 0 0
cgroup /sys/fs/cgroup/perf_event cgroup rw,nosuid,nodev,noexec,relatime,perf_event 0 0
cgroup /sys/fs/cgroup/devices cgroup rw,nosuid,nodev,noexec,relatime,devices 0 0
cgroup /sys/fs/cgroup/pids cgroup rw,nosuid,nodev,noexec,relatime,pids 0 0
cgroup /sys/fs/cgroup/cpu,cpuacct cgroup rw,nosuid,nodev,noexec,relatime,cpu,cpuacct 0 0
cgroup /sys/fs/cgroup/net_cls,net_prio cgroup rw,nosuid,nodev,noexec,relatime,net_cls,net_prio 0 0
cgroup /sys/fs/cgroup/cpuset cgroup rw,nosuid,nodev,noexec,relatime,cpuset 0 0
cgroup /sys/fs/cgroup/bio cgroup rw,nosuid,nodev,noexec,relatime,bio 0 0
systemd-1 /proc/sys/fs/binfmt_misc autofs rw,relatime,fd=25,pgrp=1,timeout=0,siipproto=5,nasproto=5,direct 0 0
debugfs /sys/kernel/debug debugfs rw,relatime 0 0
tmpfs /dev/mqueue mqueue rw,relatime 0 0
hugetlbfs /dev/hugepages hugetlbfs rw,relatime 0 0
binfmt_misc /proc/sys/fs/binfmt_misc binfmt_misc rw,relatime 0 0
vmware-vblock /run/vmtoolsd-fuse fuse.vmware-vblock rw,relatime,user_id=0,group_id=0,default_permissions,allow_other 0 0
fusectl /sys/fs/fuse/connections fusectl rw,relatime 0 0
tmpfs /run/user/133 tmpfs rw,nosuid,nodev,relatime,size=204448k,mode=700,uid=133,gid=133 0 0
tmpfs /run/user/0 tmpfs rw,nosuid,nodev,relatime,size=204448k,mode=700 0 0
gvfsd-fuse /run/user/0/gvfs fuse.gvfsd-fuse rw,nosuid,nodev,relatime,user_id=0,group_id=0 0 0
```

- Run `cat /proc/uptime` to measure the computers working time

```
root@kali:~# cat /proc/uptime
1871.97 1571.13
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Non-Volatile Data



- View connections and shared files

```
root@kali:~# smbtree
Enter root's password:
WORKGROUP\SCASC
WORKGROUP
\\WIN-NEMVGG9G3L6
\\WIN-K20VHD6N7FP
\\WIN-CQOMK62867E
\\WIN-BMCH3JB1U00
\\WIN-ARMEUMBFGA3
\\WIN-5E0MNGDMTRQ
\\USER
\\SD-011
\\SD-009
\\SD-008
\\SD-005
\\SD-004
\\S
\\S
\\S
\\S
\\R
\\R
```

```
root@kali:~# smbclient -L localhost
Enter root's password:
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 4.1.17-Debian]

Sharename      Type      Comment
-----
print$         Disk     Printer Drivers
share          Disk     IPC Service (Samba 4.1.17-Debian)
IPC$           IPC
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 4.1.17-Debian]

Server          Comment
-----
Workgroup       Master
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Non-Volatile Data (Cont'd)



Check for auto-start services

```
root@kali:~# ls /etc/rc*.d
K01apache2      K01lvm2-lvmpolld  K01sshd
K01apache-htcacheclean K01mirodo         K01tunnel4
K01atftpd       K01nmbd           K01thin
K01avahi-daemon K01openbsd-inetd  K01luidd
K01beef-sss     K01openvas-manager K02mysql
K01bluetooth    K01openvas-scanner K02postgresql
K01couchdb      K01openvpn        K04rsyslog
K01darkstat     K01pcscd          K06nfs-common
K01dnsm2tcp     K01redis-server   K06rpcbind
K01exim4        K01redsocks       README
K01gdm3         K01rsync           S01killprocs
K01greenbone-security-assistant K01sanad          S02motd
K01iodined      K01smartmontools  S06bootlogs
K01irqbalance  K01snbd           S07single
K01lvm2-lvmetad K01snmpd
K01speech-dispatcher
```

Review recently modified files

```
root@kali:~# find /etc -type f -printf '%TY-%Tm-%Td %p\n' | sort -r
2016-05-07:35:12.3554237000 /etc/machine-id
2016-05-07:32:02.9885839000 /etc/network/interfaces
2016-05-07:31:51.2542277000 /etc/NetworkManager/system-connections/Wired connect
2016-05-07:25:25.4982277000 /etc/adjtime
2016-05-07:25:23.4542277000 /etc/default/rcS
2016-05-07:25:16.3542277000 /etc/apt/sources.list
2016-05-07:25:16.1982277000 /etc/shadow
2016-05-07:25:15.4462277000 /etc/group
2016-05-07:25:14.9182277000 /etc/gshadow
2016-05-06:59:48.8822277000 /etc/default/grub
2016-05-06:55:43.9262277000 /etc/console-setup/cached_UTF-8_del.kmap.gz
2016-05-06:55:41.6822277000 /etc/console-setup/cached_Lat15-Fixed16.psf.gz
2016-05-06:55:40.9982277000 /etc/default/console-setup
2016-05-06:55:39.5982277000 /etc/init.d/depend.stop
2016-05-06:55:39.5982277000 /etc/init.d/depend.start
2016-05-06:55:39.5982277000 /etc/init.d/depend.boot
2016-05-06:55:39.3822277000 /etc/default/keyboard
2016-05-06:55:37.1622277000 /etc/localtime
2016-05-06:55:37.1342277000 /etc/timezone
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Non-Volatile Data (Cont'd)



Collect Login and System Logs

```
authlog
May 31 07:31:03 kali polkitd(authority=local): Registered Authentication Agent for unix-session:c3
[system bus name :1.37 [gnome-shell --mode=gdm], object path /org/freedesktop/PolicyKit1/
AuthenticationAgent, locale en_US.UTF-8)
May 31 07:31:05 kali realmd[1095]: Loaded settings from: /usr/lib/realmd/realmd-defaults.conf /usr/lib/
realmd/realmd-distro.conf
May 31 07:31:05 kali realmd[1095]: holding daemon: startup
May 31 07:31:05 kali realmd[1095]: starting service
May 31 07:31:05 kali realmd[1095]: connected to bus
May 31 07:31:05 kali realmd[1095]: released daemon: startup
May 31 07:31:05 kali realmd[1095]: claimed name on bus: org.freedesktop.realmd
May 31 07:32:05 kali gdm-password: pam_unix(gdm-password:session): session opened for user root by
(uid=0)
May 31 07:32:05 kali systemd-logind[593]: New session 1 of user root.
May 31 07:32:05 kali systemd: pam_unix(systemd-user:session): session opened for user root by (uid=0)
May 31 07:32:06 kali realmd[1095]: quitting realmd service after timeout
May 31 07:32:06 kali realmd[1095]: stopping service
May 31 07:32:09 kali polkitd(authority=local): Registered Authentication Agent for unix-session:1
[system bus name :1.62 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/
AuthenticationAgent, locale en_US.UTF-8)
May 31 07:35:01 kali CRON[1561]: pam_unix(cron:session): session opened for user root
May 31 07:35:01 kali CRON[1561]: pam_unix(cron:session): session closed for user root
May 31 07:39:01 kali CRON[1602]: pam_unix(cron:session): session opened for user root
May 31 07:39:02 kali CRON[1603]: pam_unix(cron:session): session closed for user root
May 31 07:45:01 kali CRON[1643]: pam_unix(cron:session): session opened for user root
May 31 07:45:01 kali CRON[1643]: pam_unix(cron:session): session closed for user root
May 31 07:55:01 kali CRON[1657]: pam_unix(cron:session): session opened for user root
May 31 07:55:01 kali CRON[1657]: pam_unix(cron:session): session closed for user root
May 31 08:03:14 kali sudo: root : TTY=pts/0 : PWD=/root : USER=root : COMMAND=ls
```

```
root@kali:~# cat /var/log/kern.log
May 30 03:22:42 kali NetworkManager[552]: <info> [1464592962.9617] address 192.168.0.184
May 30 03:22:42 kali NetworkManager[552]: <info> [1464592962.9627] plen 24 (255.255.255.0)
May 30 03:22:42 kali NetworkManager[552]: <info> [1464592962.9627] gateway 192.168.0.1
May 30 03:22:42 kali NetworkManager[552]: <info> [1464592962.9627] server identifier 192.168.0
May 30 03:22:42 kali NetworkManager[552]: <info> [1464592962.9627] lease time 3600
May 30 03:22:42 kali NetworkManager[552]: <info> [1464592962.9627] hostname 'kali'
May 30 03:22:42 kali NetworkManager[552]: <info> [1464592962.9627] nameserver '192.168.0.8'
May 30 03:22:42 kali NetworkManager[552]: <info> [1464592962.9841] dhcp4 [eth0]: state changed b
bound -> bound
May 30 03:47:18 kali NetworkManager[552]: <info> [1464594438.5549] address 192.168.0.184
May 30 03:47:18 kali NetworkManager[552]: <info> [1464594438.5550] plen 24 (255.255.255.0)
May 30 03:47:18 kali NetworkManager[552]: <info> [1464594438.5550] gateway 192.168.0.1
May 30 03:47:18 kali NetworkManager[552]: <info> [1464594438.5550] server identifier 192.168.0
May 30 03:47:18 kali NetworkManager[552]: <info> [1464594438.5550] lease time 3600
May 30 03:47:18 kali NetworkManager[552]: <info> [1464594438.5551] hostname 'kali'
May 30 03:47:18 kali NetworkManager[552]: <info> [1464594438.5551] nameserver '192.168.0.8'
May 30 03:47:18 kali NetworkManager[552]: <info> [1464594438.6348] dhcp4 [eth0]: state changed b
bound -> bound
May 30 04:15:01 kali NetworkManager[552]: <info> [1464596101.4367] address 192.168.0.184
May 30 04:15:01 kali NetworkManager[552]: <info> [1464596101.4368] plen 24 (255.255.255.0)
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Non-Volatile Data (Cont'd)



- Search for files with strange names in **/dev** directory

- Check security settings of the system for anomalies

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# rkhunter --check --two  
Warning: Suspicious file types found in /dev:  
/dev/shm/pulse-shm-1757356222: data  
/dev/shm/pulse-shm-2552238486: data  
/dev/shm/pulse-shm-269953325: data  
/dev/shm/pulse-shm-3108731619: data  
/dev/shm/pulse-shm-821688646: data  
/dev/shm/pulse-shm-1355211844: data  
/dev/shm/pulse-shm-1764722882: data  
/dev/shm/pulse-shm-2702859299: data  
/dev/shm/pulse-shm-2625548305: data  
/dev/shm/pulse-shm-689540227: data  
/dev/shm/pulse-shm-3585489933: data  
/dev/shm/pulse-shm-65350776: data  
root@kali:~#
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# chkrootkit  
ROOTDIR is '/'  
Checking 'amd'... not found  
Checking 'basenane'... not infected  
Checking 'biff'... not found  
Checking 'chfn'... not infected  
Checking 'chsh'... not infected  
Checking 'cron'... not infected  
Checking 'crontab'... not infected  
Checking 'date'... not infected  
Checking 'du'... not infected  
Checking 'dirname'... not infected  
Checking 'echo'... not infected  
Checking 'egrep'... not infected  
Checking 'env'... not infected  
Checking 'find'... not infected  
Checking 'fingerd'... not found  
Checking 'gpm'... not found  
Checking 'grep'... not infected  
Checking 'hdparm'... not infected  
Checking 'su'... not infected  
Checking 'ifconfig'... not infected  
Checking 'inetd'... not infected
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Non-Volatile Data (Cont'd)



- Find the deleted files and associated data

- Use Linux Volume Manager (LVM) to detect unallocated partitions and files

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# file -d TestRawImage.dd  
d/d * 7: More Icons  
r/r * 34: Shakira- --Sale El Sol mix 2011(BEST LATINO MUSIC HITS).mp4  
d/d * 36: Old Melodies  
d/d * 43: 0  
d/d * 43: P  
d/d * 45: P  
d/d * 48: R  
d/d * 50: R  
d/d * 54: S  
d/d * 56: S  
d/d * 58: N  
d/d * 60: K  
d/d * 62: L  
r/r * 68: 1  
r/r * 73: 0  
r/r * 77: 0  
r/r * 82: 0  
r/r * 87: 0  
r/r * 92: 0  
r/r * 96: 0  
root@kali:~#
```

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# parted  
GNU Parted 3.2  
Using /dev/sda  
Welcome to GNU Parted! Type 'help' to view a list of commands.  
(parted) print free  
Model: Mott Virtual Disk (scsi)  
Disk /dev/sda: 26.8GB  
Sector size (logical/physical): 512B/4096B  
Partition Table: msdos  
Disk Flags:  


| Number | Start  | End    | Size   | Type     | File system     | Flags |
|--------|--------|--------|--------|----------|-----------------|-------|
| 1      | 32.3kB | 1049kB | 1016kB | primary  | ext4            | boot  |
| 2      | 25.7GB | 25.7GB | 1048kB | extended | Free Space      |       |
| 5      | 25.7GB | 26.8GB | 1140MB | logical  | linux-swaps(v1) |       |
|        | 26.8GB | 26.8GB | 1049kB |          | Free Space      |       |


  
(parted)
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


Investigators need detailed information and evidences to solve the case with ease. The above commands provide ample information about the non-volatile data on a Linux machine. The investigator can decide which information needs to be extracted from the configuration files, or which information about (or from) files needs to be collected for additional analysis because in some cases the attacker could be actively logged into the system during the investigation. In such cases, the investigator may decide to track the attacker.

The investigator must also preserve certain important information from being modified or deleted. This includes safeguarding the non-volatile information of the system, including firewall logs, swap files, antivirus logs, slack space, and unallocated drive space. To preserve the integrity of the evidence, a chain of custody is prepared and the collected evidence is documented for further investigation.


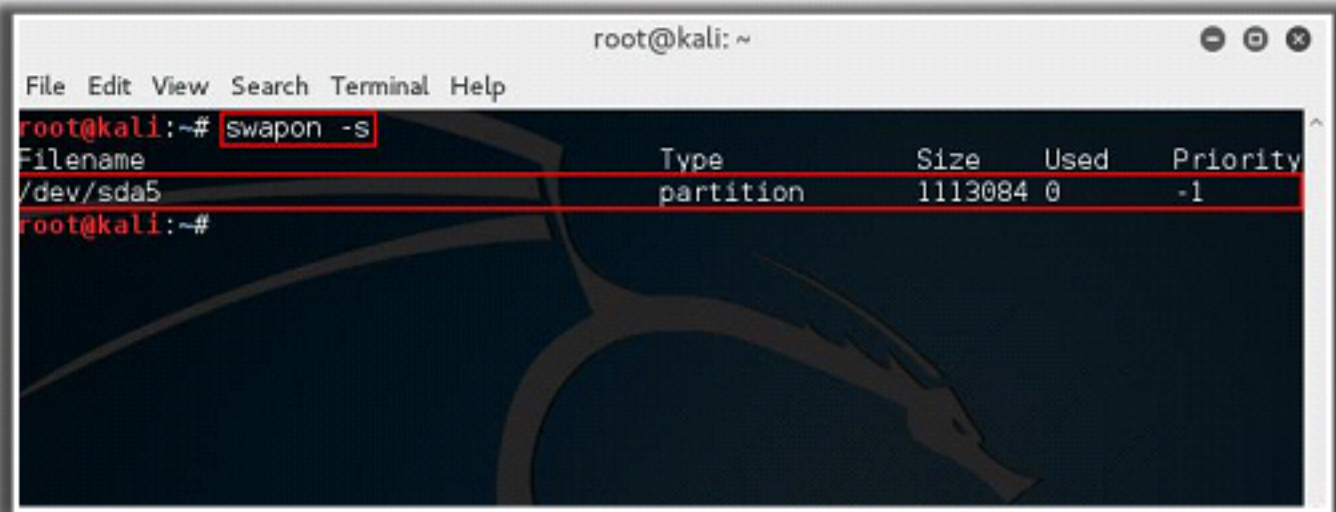

Swap Space



- A swap space is a storage space on a hard disk used as the **virtual memory extension** of a computer's RAM
- When the applications running on Linux machines use up the RAM memory, the inactive pages inside it move to the swap space to free up the memory



- The Slack space on a hard disk should be twice the physical RAM, if the RAM size is $\leq 2\text{GB}$
- In case the physical RAM is more than 2GB, for instance 5 GB, the slack space on a hard disk should be 2 GB more than the Physical RAM, i.e., $5+2=7\text{ GB}$
- Issue **swapon -s** command to view the swap space



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# swapon -s  
Filename                                Type      Size      Used      Priority  
/dev/sda5                               partition 1113084 0         -1  
root@kali:~#
```

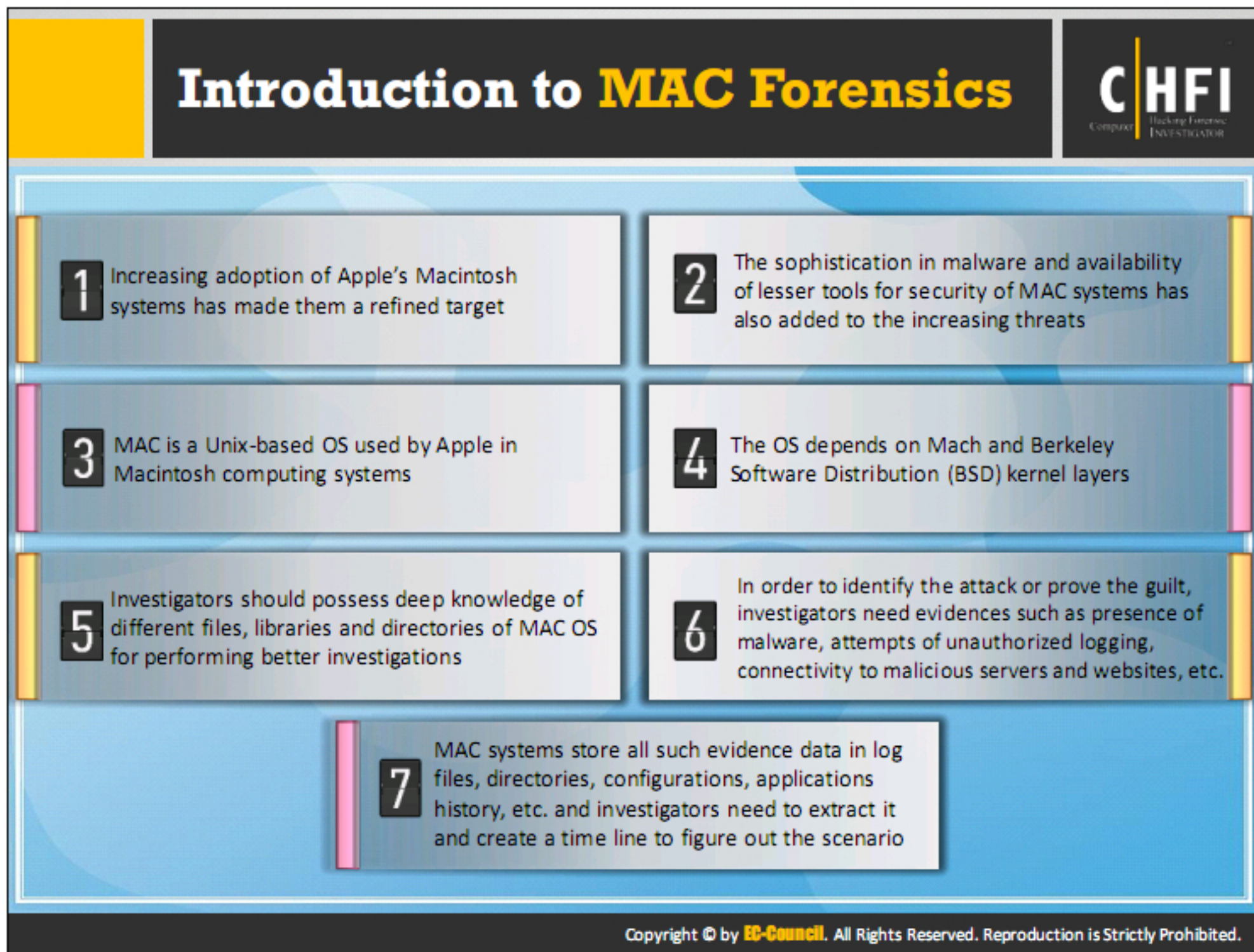
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Linux operating system allocates certain amount of storage space on a hard disk called Swap Space. OS uses as the virtual memory extension of a computer's real memory (RAM). The OS splits physical RAM into bits/chunks of memory called pages. Having a swap space allows your computer's operating system to pretend that you have more RAM than you actually do. The least recently used pages in RAM can be "swapped out" to your hard disk until they are needed later, so that new files can be "swapped in" to RAM. In larger operating systems (such as IBM's OS/390), the swapping is called paging.

One advantage of a swap space is, the ability to organize itself as a single contiguous space so that the system can operate it using fewer I/O operations to read or write a complete file. In general, Windows and UNIX-based operating systems provide a default swap space of a certain size that the user or a system administrator can change.



Mac is short for the Macintosh operating systems developed by Apple to support its line of devices and series of personal computers. Mac is one of the most adopted systems across the globe and is also facing increase in number of attacks annually. The investigators must have knowledge of Mac, its process, policies, functions and internal storage patterns used by the operating system to be able to perform forensics. This section will help introduce you with the processes that can help to conduct forensics investigation over a Mac-based system.



The usage of Apple products has increased drastically in the last few years, for instance MAC computers, iPods, iPads, iPhones etc. Eventually they have also become the main target to the cyber attackers. The reason behind this is, there are not enough security tools developed to defend these attacks. MAC Forensics comes into picture when there is an attack on Macintosh systems.

MAC forensics refers to investigation of a crime occurred on or using a MAC device. To encounter the cyber-attacks, it is indispensable that the forensic investigators possess a good understanding on the MAC file system and all the operating system features. MAC operating system works on HFS (Hierarchical File System) File structure, and presently HFS+ is the most preferred file system used in MAC OS devices.

MAC Forensics Data



Find the System Version:

- Identify the system version by viewing the **SystemVersion.plist** file located at:
/System/Library/CoreServices/SystemVersion.plist

Timestamp:

- Helps investigator to calculate the uptime of the system, correlate log events and build a timeline
- Provides important info such as creation, access and modification times of any file
- Gather timestamps of applications, services, events and logs of the system
- Use the command line input **stat** to see the timestamp of any file
- Usage: **stat [-Flnqrsx] [-f format] [-t timefmt] [file ...]**

Application bundles:

- Special directories that store application data, hidden from the user
- Investigators can analyze these bundles to identify malware or other suspicious data
- Evaluate the executable codes to find if something is wrong with the application

Finder:

- Default Mac application that helps find specific files and folders
- Helps to sort in the required order

```
Pazzer@Hammerhead:~$ stat -x /Users/Hammerhead/Documents/Puzzle/Downloads/kubuntu-16.04-desktop-amd64.iso
File: "/Users/Hammerhead/Documents/Puzzle/Downloads/kubuntu-16.04-desktop-amd64.iso"
Size: 1528762880  FileType: Regular File
Mode: (0644/-rw-r--r--)  UID: ( 501/Hammerhead)  GID: ( 20/ staff)
Device: 1,4  Inode: 8668764  Links: 1
Access: Sat Jun 25 19:02:32 2016
Modify: Fri Jun 3 14:54:49 2016
Change: Fri Jun 3 14:54:49 2016
Pazzer@Hammerhead:~$
```

```
Pazzer@Hammerhead:~$ cat /System/Library/CoreServices/SystemVersion.plist
<?xml version="1.0" encoding="UTF-8"?>
<dict>
  <key>ProductBuildVersion</key>
  <string>15F34</string>
  <key>ProductCopyright</key>
  <string>1983-2016 Apple Inc.</string>
  <key>ProductModel</key>
  <string>Mac OS X</string>
  <key>ProductUserVisibleVersion</key>
  <string>10.11.5</string>
  <key>ProductVersion</key>
  <string>10.11.5</string>
</dict>
</plist>
Pazzer@Hammerhead:~$
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Forensics Data (Cont'd)



User account

- Gather the data related to all the user accounts such as **user IDs**, **passwordpolicyoption**, etc.
- Help to find the guest and administrator users
- Location about the user account data is stored in a user Library folder - **/Users/username/Library**
- Collect information such as access, modification, and creation for each account

Analyze file systems

- MAC OS uses the **HFS+ file system**, whose header stores file system data, such as allocation block size, volume, creation timestamp, and the location
- Has a header of 1024bytes and allocation blocks, each with size of 4K bytes
- Comprises data streams called forks, which include data fork and resource fork
- Data fork stores file content, while resource fork consists file information

Basic Security Module (BSM)

- Saves file information and related events using a **token**, which has binary structure
- The token represents specific data, such as **arguments of the program**, **return value**, **text data**, **socket**, **execution**, **action in a file**, etc.
- Data stored in BSM helps to determine file type, creator, and usage data

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Forensics Data (Cont'd)



1 Spotlight

- An integrated search technology that helps users to search for specific keywords within files
- Finds any known **suspicious files** and **applications**
- Use a spotlight to search for specific keywords that represent malice.

2 Time machine

- It is a backup tool that stores hard disk contents
- Comprises **BackupAlias** file containing information, in a binary format, about the hard disk used to store the backups

3 Home directory

- Stores the authentication data, such as logon attempts both success and failure of all users
- Helps investigator in determining all the attempts made to bypass the security along with the timestamps
- Also stores application and installation folders
- Other files include desktop, documents, library, magazines, etc.

4 Kexts

- MAC OS can load additional capabilities by loading kernel extensions
- Analyze the system for kernel extensions



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Forensics Data (Cont'd)



Apple Mail

- The default email application with multiple POP3 and IMAP account support and advanced filtering
- Stores user email in the directory: **/Users//Library/Mail**
- Stores email in eml format, where each email is its own file in ASCII format
- Use email extractors such as Email Extractor 7, Data Extractor, etc.

Instant Messengers

- MAC comes with default IM application iChat, which does not store previous conversations, but users can choose to save them manually
- Check for any saved chats in the default location: **/Users/<username>/Documents/iChats**
- The individual applications are stored as **<username>** on **<date>** at **<time>.ichat**

Web browsers

- Safari is the default browser on a Mac system
- Information such as browsing history, download history, and bookmarks can assist as evidence and is stored as History.plist, Downloads.plist, and Bookmarks.plist respectively in the **/Users//Library/Safari** location


Command line inputs

- MAC OS records commands in bash shell and stores the in the file **.bash_history**
- Use the command **\$tail .bash_history** to view the last commands




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Forensics Data (Cont'd)




Property list or plist

- Mac OS store user settings in the form of Property List Format file (plist file)
- Stores settings data in the form of Core Foundation types including **CFString**, **CFNumber**, **CFBoolean**, **CFDate**, **CFData**, **CFArray** and **CFDictionary**
- Uses XML or binary data format to store data




Network kernel extensions

- Modify the networking infrastructure of OS X for connecting with the external networks or servers
- Help in **creating modules** that can be dynamically placed across the network to monitor and modify network traffic as well as receive notification of asynchronous events
- Modules can **stop transfer** of the **network packets**, **manipulate incoming or outgoing packet data**, or **sniff traffic on specific interfaces**
- Gather the data from extensions and look for suspicious connections



Keychain

- Built-in password manager that **saves the credentials** for **websites**, **wireless networks**, **SSH servers**, **private keys**, etc.
- Stores the credentials in an encrypted (3DES) container that can unlock only with the master password
- Can store sensitive information required for investigation



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

With the increase of the usage of Apple's Macintosh systems, the number attacks have increased tremendously. If a MAC device is present in the crime scene, seize the device at first the device and safeguard it. The suspect device is then imaged using Write blockers and the investigations are performed on the imaged copy. Forensic examiners then examine the digital media in a forensically sound manner. Their task is to identify, preserve, recover, analyze and present the evidences extracted from them in the court if law.

We have covered all the sources which are of forensic concern and from which the investigators can retrieve information in a MAC operating system. For instance the Version.plist file which contains the system version details, the Timestamp utility which helps the investigator to correlate the log events, Application bundles which are directory hierarchies that consists of sub folders that contain executable code, etc. Analyzing all these sources can provide crucial forensic data, which may help the investigators to trace out the attackers.

Investigators can procure all the user account details from the Library folder and can gather information related to the account creation, modification, and access timings. It is essential for forensic investigators to have a good understanding of the file system of the device he/she is dealing with. As we are discussing about Apple's Macintosh systems, the newer versions of MAC OS use HFS+ file system. In depth understanding of the data structure and allocation blocks will helps the investigator to find out the required forensic information. The MAC OS uses the Basic Security Model, which helps to understand the file type, its creator and data usage.

Spotlight is a desktop search feature of the MAC OS, which indexes the files by their types and thus making the search easy. This technology is particularly useful for investigators to trace a specific file.

The Home folder in the MAC OS X stores all the files, documents, applications, library folders etc., pertaining to a particular user. The MAC OS creates separate Home directory for each user of the system with their username; so that the investigator can easily analyze the Home directory and retrieve crucial data such as passwords, log files, library folders, logon attempts, and other forensically important information.

MAC OS has its default standalone email client called the Apple mail. It stores all the email messages on the host computer. These email messages can act as crucial source of forensic evidences. Safari is the default web browser in the MAC system. It holds information of the browsing history, download history, etc. as plist files in the Library folder.

MAC Log Files



Log File	Uses
/var/log/crashreporter.log	Application crash history on crash
/var/log/cups/access_log	Printer Connection Information
/var/log/cups/error_log	Printer Connection Information
/var/log/daily.out	Network Interface History
/var/log/samba/log.nmbd	Samba (Windows based machine) connection information
~/Library/Logs	Home directory specific application logs
~/Library/Logs/ iChatConnectionErrors	iChat connection information
~/Library/Logs/Sync	Information of devices on .Mac syncing
/var/log/*	System Log files main folder
/var/audit/*	Audit Log
/var/log/install.log	Install date of system and software updates

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


MAC Directories











File name	Location
Launch Agents files	/Library/LaunchAgents/*, /System/Library/LaunchAgents/*
Launch Daemons files	/Library/LaunchDaemons/*, /System/Library/LaunchDaemons/*
Startup Items file	/Library/StartupItems/*, /System/Library/StartupItems/*
Mac OS X jobs	/usr/lib/cron/jobs/*
Cron tabs or scheduled jobs	/etc/crontab, /usr/lib/cron/tabs/*
Wireless networks	/Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist
User preference settings for applications and utilities	%%users.homedir%%/Library/Preferences/*
Attached iDevices	%%users.homedir%%/Library/Preferences/com.apple.iPod.plist
Social Accounts	%%users.homedir%%/Library/Accounts/Accounts3.sqlite
Trash directory	%%users.homedir%%/.Trash/
Safari Main Folder	%%users.homedir%%/Library/Safari/*
Mozilla Firefox web browser	%%users.homedir%%/Library/Application Support/Firefox/*
Google Chrome web browser	%%users.homedir%%/Library/Application Support/Google/Chrome/*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Forensics Tools



 OS X Auditor- Mac Forensics Tool http://www.sectecho.com	 F-Response https://www.f-response.com
 MacForensicLab http://www.secureindia.in	 Mac OS X Memory Analysis Toolkit https://github.com
 Memoryze for the Mac https://www.fireeye.com	 Volatility 2.5 http://www.volatilityfoundation.org
 Mac Marshal http://www.appleexaminer.com	 OS X Rootkit Hunter for Mac http://download.cnet.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

OS X Auditor- Mac Forensics Tool

Source: <http://www.sectecho.com>

OS X Auditor is a python based computer forensics tool. The tool allows analysts to parse and hash artifacts on the running system or a copy of a system to not modify the original evidence.

MacForensicLab

Source: <http://www.secureindia.in>

MacForensicsLab is a forensic tool that allows examiners to conduct their examinations and process suspect data to find and recover deleted and embedded files – then preview and recover them.

Memoryze for the Mac

Source: <https://www.fireeye.com>

Memoryze for the Mac is free memory forensic software that helps incident responders find evil in memory on Macs. Memoryze for the Mac can acquire and/or analyze memory images. Analysis can be performed on offline memory images or on live systems.

Mac Marshal

Source: <http://www.appleexaminer.com>

Mac Marshal is a tool to analyze Mac OS X file system images. It scans a Macintosh disk image, automatically detects, and displays Macintosh and Windows operating systems and virtual

machine images, then runs a number of analysis tools on the image to extract Mac OS X-specific forensic evidence written by the OS and common applications.

F-Response

Source: <https://www.f-response.com>

F-Response is a software utility that enables investigators to conduct live Forensics, Data Recovery, and eDiscovery over an IP network using their tool(s) of choice. It provides read-only access to full physical disk(s), physical memory (RAM), 3rd party Cloud, Email and Database storage.

Mac OS X Memory Analysis Toolkit

Source: <https://github.com>

Mac OS X Memory Analysis Toolkit is an open source toolkit for Mac OS X and BSD forensics. The tool is a python based and allows investigating security incidents and finding information for malwares and any malicious program on the system.

Volatility 2.5

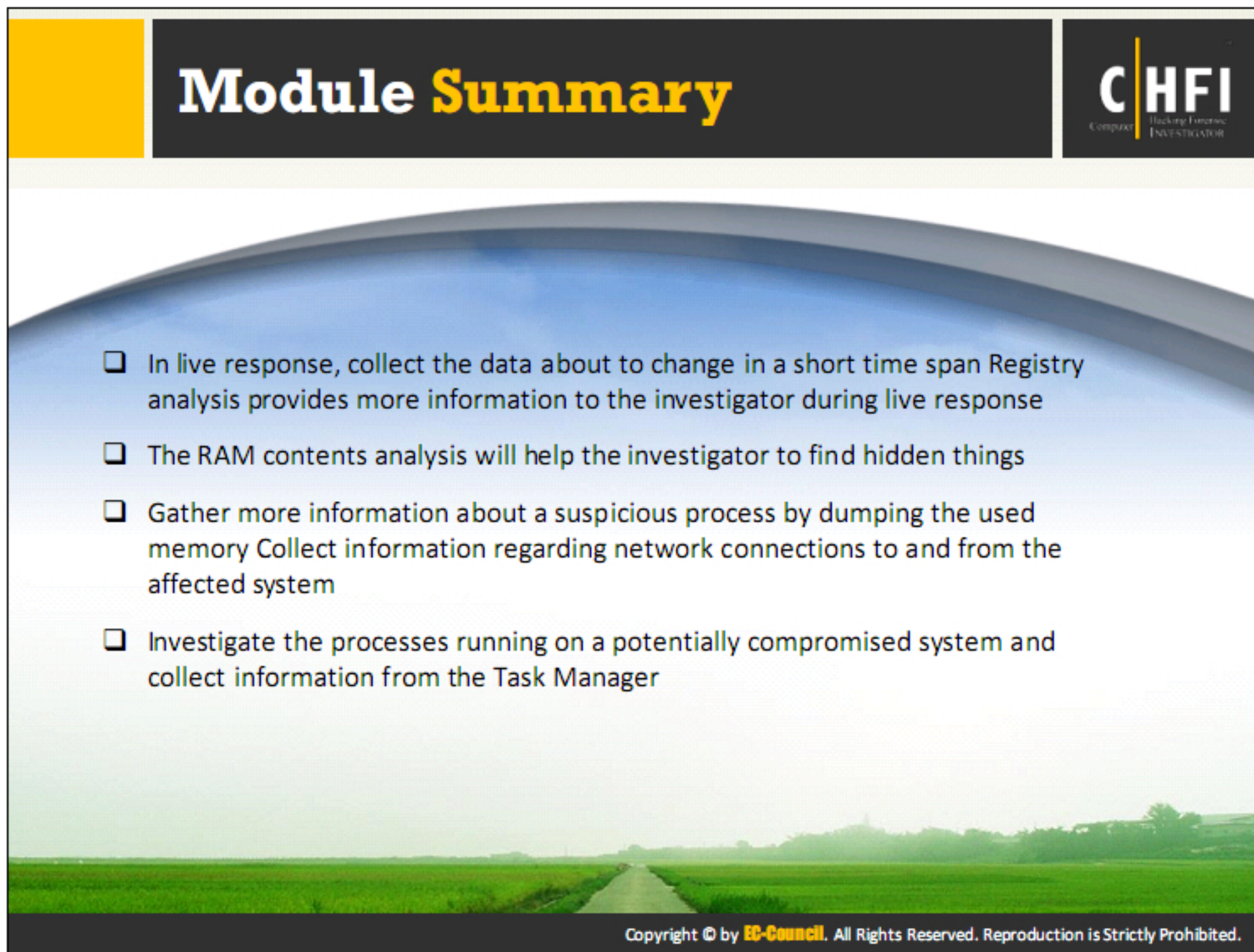
Source: <http://www.volatilityfoundation.org>

Volatility Framework is a memory analysis and forensics tools used for finding contraband within hard drive images. Volatility enables users to analyze the runtime state of a system using the data found in volatile storage (RAM).


OS X Rootkit Hunter for Mac

Source: <http://download.cnet.com>

OS X Rootkit Hunter is scanning tool that can detect malicious tools on a Mac. This tool scans for rootkits, backdoors, and local exploits.



Module Summary



- ☐ In live response, collect the data about to change in a short time span Registry analysis provides more information to the investigator during live response
- ☐ The RAM contents analysis will help the investigator to find hidden things
- ☐ Gather more information about a suspicious process by dumping the used memory Collect information regarding network connections to and from the affected system
- ☐ Investigate the processes running on a potentially compromised system and collect information from the Task Manager

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

In this module, we have covered the various aspects of operating system forensics of the three critical operating systems that are most likely to be encountered by forensic investigators, i.e. Windows, Mac and Linux OSs. We discussed the importance of collecting volatile information in the Windows system that provides crucial information such as system time, logged-on users, network information, mapped drives etc., as well as non-volatile information such as documents, spread sheets, etc., that reside on the hard disk of the computer.

Analyzing Windows Registry is an important part of forensic investigations as it contains forensically valuable information on the list of active user profiles, configuration information, hardware and software settings of the system, etc. The MRU lists are present in different locations of the Registry Editor, which records all the recent activities of the users of the system.

The different shell commands of the Linux OS retrieves crucial data that helps the investigators in finding out the source and time of the attack. Analyzing the Linux log files provide key information regarding failed login attempts, printer logs, server logs etc.

To perform forensic investigation on a MAC system, an investigator should have a good understanding on the files system, and the various operating system features. The BSM consists of tokens that hold the typical file information and related events, which gives access to information such as arguments of the program, return value, text data, socket, execution, action in a file, etc.