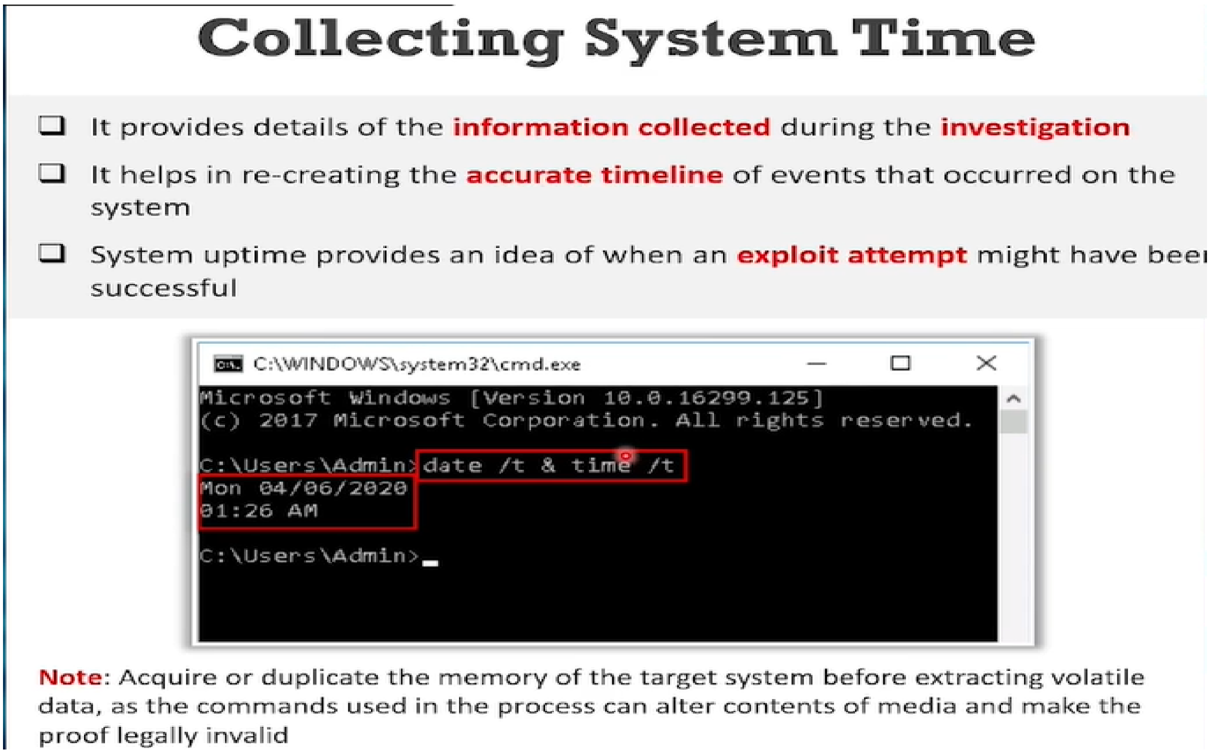
Digital Forensics

Windows forensics

1)



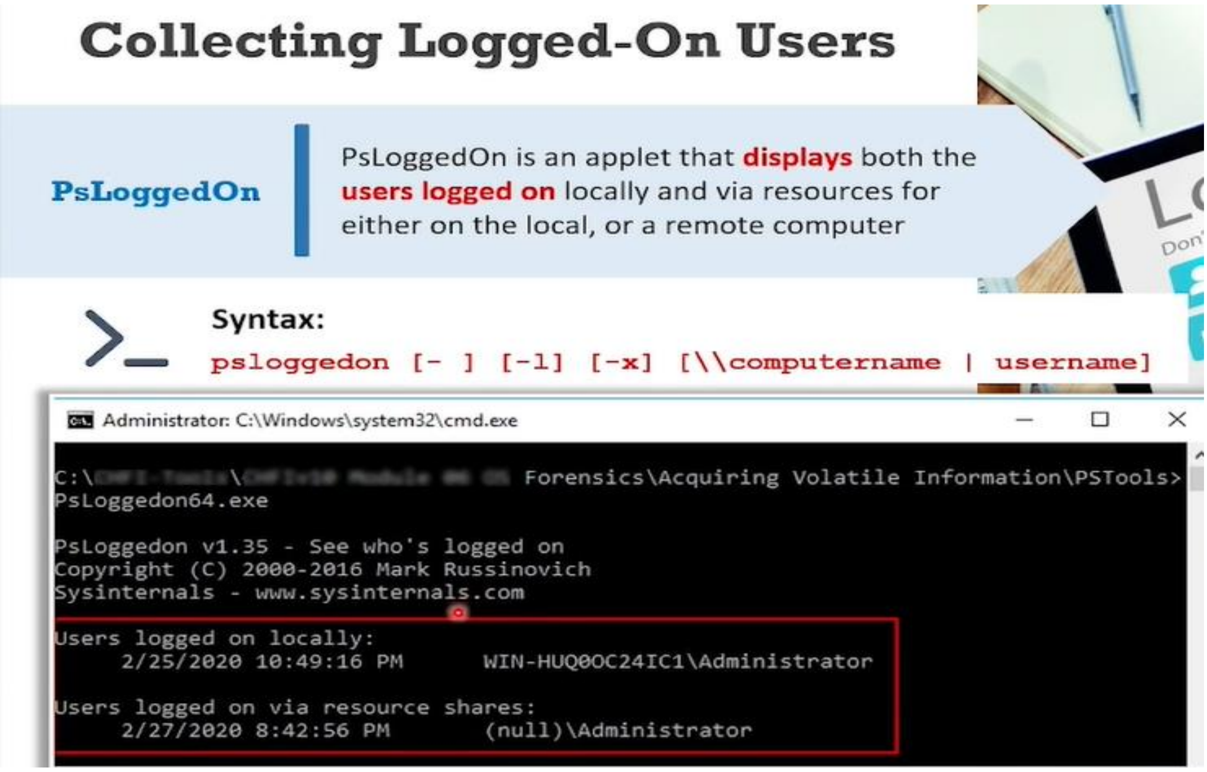
Collecting System Time

- □ It 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

```
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Admin>date /t & time /t
Mon 04/06/2020
01:26 AM

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

2)



Collecting Logged-On Users

PsLoggedOn

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:\[redacted]\[redacted] Forensics\Acquiring Volatile Information\PSTools>
PsLoggedon64.exe

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
     2/25/2020 10:49:16 PM       WIN-HUQ0OC24IC1\Administrator

Users logged on via resource shares:
     2/27/2020 8:42:56 PM        (null)\Administrator
```

3)

Collecting Logged-On Users (Cont'd)

LogonSessions Tool

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

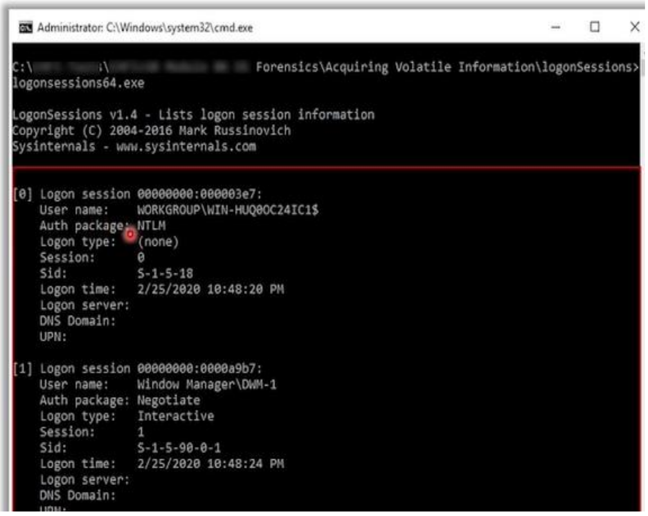
Syntax:

```
logonsessions [-c[t]] [-p]
```

-c, Print output as CSV

-ct, Print output as tab-delimited values

-p, List processes running in logon session



```
C:\[redacted]\[redacted] Forensics\Acquiring Volatile Information\logonSessions>
logonsessions64.exe

LogonSessions v1.4 - Lists logon session information
Copyright (C) 2004-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
    User name:    WORKGROUP\WIN-HUQ0OC24IC1$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   2/25/2020 10:48:20 PM
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:0000a9b7:
    User name:    Window Manager\DWM-1
    Auth package: Negotiate
    Logon type:   Interactive
    Session:      1
    Sid:          S-1-5-90-0-1
    Logon time:   2/25/2020 10:48:24 PM
    Logon server:
    DNS Domain:
```

4)

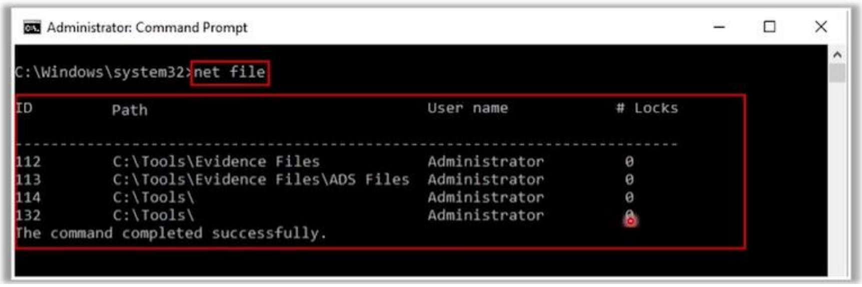
Collecting Open Files: net file Command

Collect **information about the files opened** by the intruder using remote login

net file 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]]
```

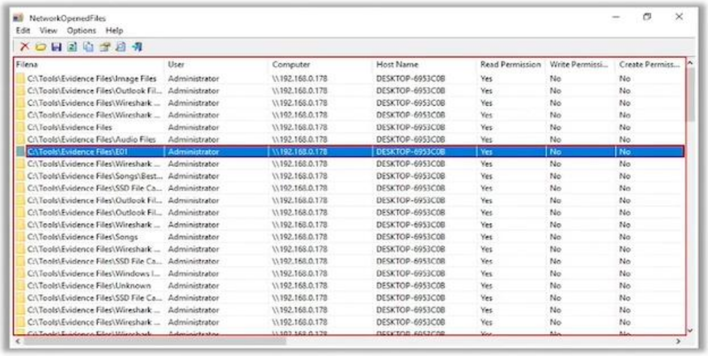


```
C:\Windows\system32>net file

ID         Path                              User name            # Locks

-------------------------------------------------------------------------------
112        C:\Tools\Evidence Files           Administrator        0
113        C:\Tools\Evidence Files\ADS Files Administrator        0
114        C:\Tools\                         Administrator        0
132        C:\Tools\                         Administrator        0
The command completed successfully.
```

5)

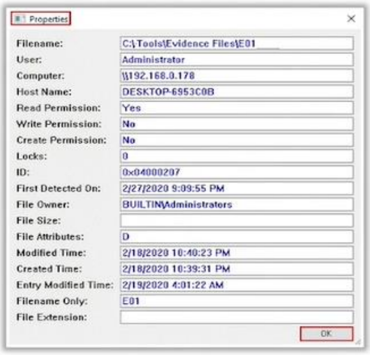
Collecting Open Files: Using NetworkOpenedFiles

- ❑ **NetworkOpenedFiles** is a utility for Windows OS that lists all the files currently **opened on the host system** through remote login
- ❑ It displays the Filename, Computer and Username, Permission information (Read/Write/Create), Locks count, File Size, File Attributes, etc.



NetworkOpenedFiles

Filena	User	Computer	Host Name	Read Permission	Write Permissi...	Create Permiss...
C:\Tools\Evidence Files\Image Files	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Outlook Fil...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Audio Files	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\E01	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Songs\Best...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\SSD File Ca...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Outlook Fil...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Outlook Fil...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Songs	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\SSD File Ca...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Windows I...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Unknown	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\SSD File Ca...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No



Properties

Filename:	C:\Tools\Evidence Files\E01
User:	Administrator
Computer:	\\192.168.0.178
Host Name:	DESKTOP-6953C0B
Read Permission:	Yes
Write Permission:	No
Create Permission:	No
Locks:	0
ID:	0x04000207
First Detected On:	2/27/2020 9:09:55 PM
File Owner:	BUILTIN\Administrators
File Size:	
File Attributes:	D
Modified Time:	2/18/2020 10:40:23 PM
Created Time:	2/18/2020 10:39:31 PM
Entry Modified Time:	2/19/2020 4:01:22 AM
Filename Only:	E01
File Extension:	

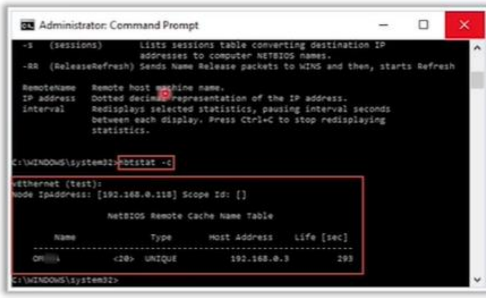
6)

Collecting Network Information

- ❑ Intruders after gaining access to a remote system, try to **discover other systems** that are available on the network
- ❑ 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

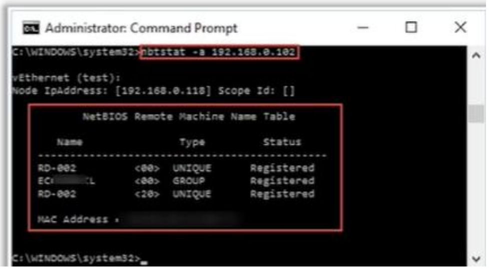
Syntax:

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



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     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.

C:\WINDOWS\system32>nbtstat -c

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

                  NetBIOS Remote Cache Name Table

        Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    [redacted]         <20>  UNIQUE          192.168.0.3         293

C:\WINDOWS\system32>
```



Administrator: Command Prompt

```
C:\WINDOWS\system32>nbtstat -a 192.168.0.102

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

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    RD-002         <00>  UNIQUE      Registered
    [redacted]     <00>  GROUP       Registered
    RD-002         <20>  UNIQUE      Registered

    MAC Address = [redacted]

C:\WINDOWS\system32>_
```

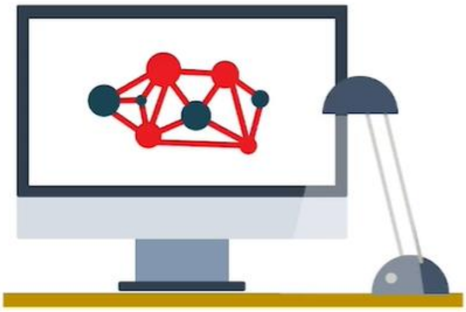
7)

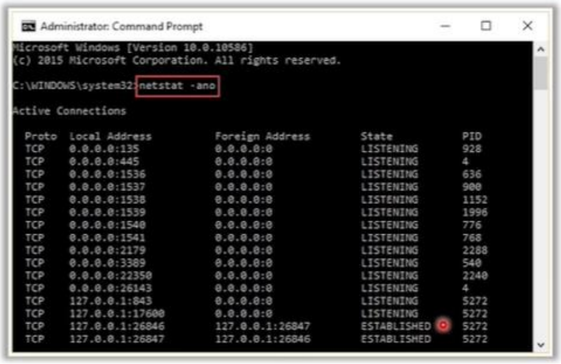
Collecting Information about Network Connections

- ❑ Collecting information about the network connections running to and from the victim system 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

Syntax:

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





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

C:\WINDOWS\system32>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       928
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1536           0.0.0.0:0              LISTENING       636
  TCP    0.0.0.0:1537           0.0.0.0:0              LISTENING       900
  TCP    0.0.0.0:1538           0.0.0.0:0              LISTENING       1152
  TCP    0.0.0.0:1539           0.0.0.0:0              LISTENING       1996
  TCP    0.0.0.0:1540           0.0.0.0:0              LISTENING       776
  TCP    0.0.0.0:1541           0.0.0.0:0              LISTENING       768
  TCP    0.0.0.0:2179           0.0.0.0:0              LISTENING       2288
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       540
  TCP    0.0.0.0:22350          0.0.0.0:0              LISTENING       2240
  TCP    0.0.0.0:26143          0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:843          0.0.0.0:0              LISTENING       5272
  TCP    127.0.0.1:17600        0.0.0.0:0              LISTENING       5272
  TCP    127.0.0.1:26846        127.0.0.1:26847        ESTABLISHED     5272
  TCP    127.0.0.1:26847        127.0.0.1:26846        ESTABLISHED     5272
```

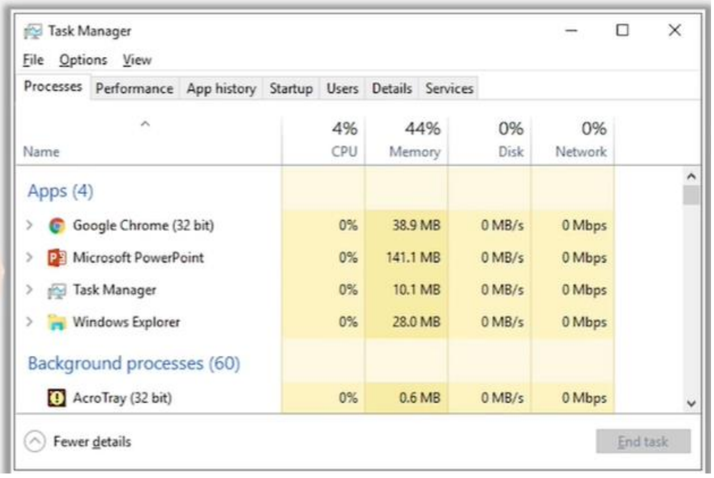
9)

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



Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
End task

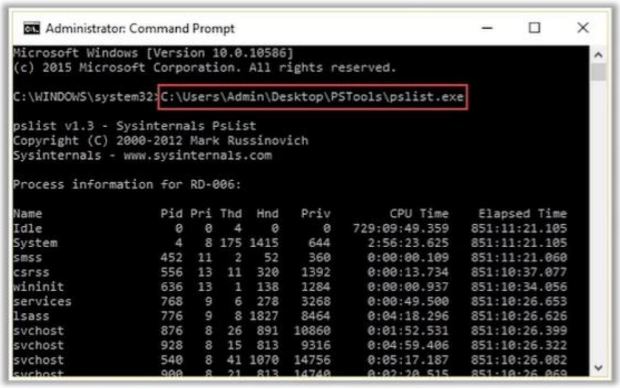
Name	4% CPU	44% Memory	0% Disk	0% Network
Apps (4)				
Google Chrome (32 bit)	0%	38.9 MB	0 MB/s	0 Mbps
Microsoft PowerPoint	0%	141.1 MB	0 MB/s	0 Mbps
Task Manager	0%	10.1 MB	0 MB/s	0 Mbps
Windows Explorer	0%	28.0 MB	0 MB/s	0 Mbps
Background processes (60)				
AcroTray (32 bit)	0%	0.6 MB	0 MB/s	0 Mbps

10)

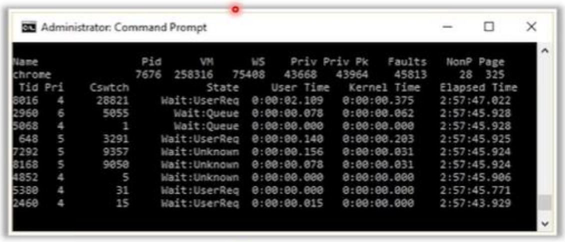
Process Information (Cont'd)

PsList

- ❑ PsList displays elementary information about all the processes running on a system
- ❑ -x switch shows processes, memory information, and threads



```
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  Hnd   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     0:00:00.109   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     0:04:18.296   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   851:10:26.082
svchost             900   8  21  813  14740     0:02:20.515   851:10:26.069
```

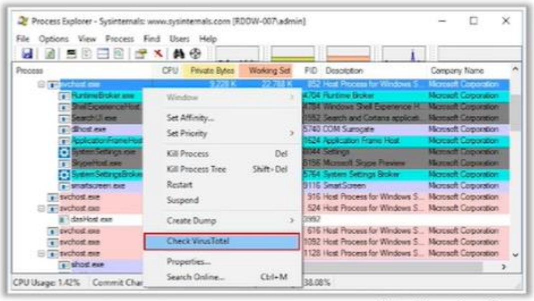


```
Name                 Pid      VM      WS    Priv Priv Pk   Faults   NonP Page
chrome              7676  258316   75408   43668   43964    45813     28  325
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
8016   4     28821     Wait:UserReq  0:00:02.109   0:00:00.375    2:57:47.022
2960   6      5055       Wait:Queue  0:00:00.078   0:00:00.062    2:57:45.928
5068   4         1       Wait:Queue  0:00:00.000   0:00:00.000    2:57:45.928
 648   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
2460   4        15     Wait:UserReq  0:00:00.015   0:00:00.000    2:57:43.929
```

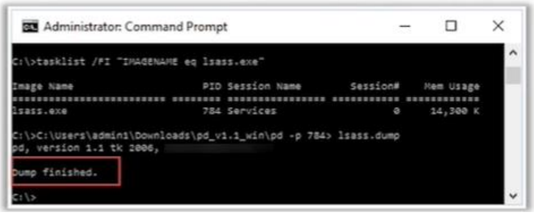
11)

Examining Process Memory

- ❑ Running processes could be **suspicious** or **malicious** in nature
- ❑ **Process Explorer** can be used to check if the process is malicious/suspicious
- ❑ Process Explorer shows 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 **ProcDump** and **Process Dumper**
- ❑ The tool comes with built-in VirusTotal support to check whether the running process is malicious

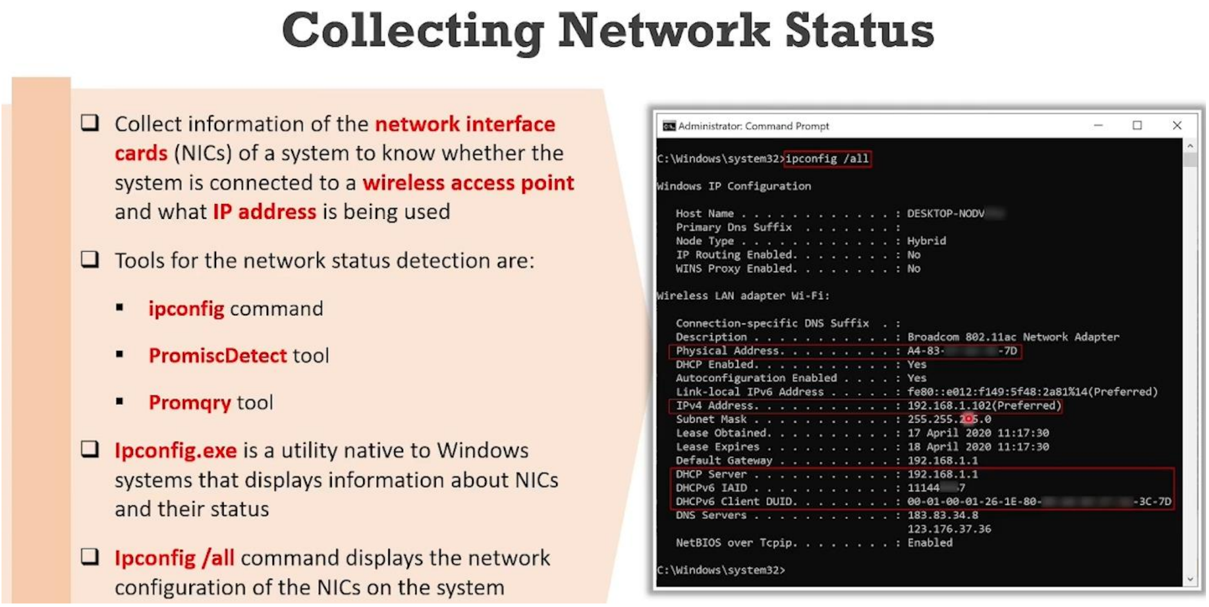


https://docs.microsoft.com



```
C:\>tasklist /FI "IMAGENAME eq lsass.exe"

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
lsass.exe                      784 Services                   0     14,300 K

C:\>C:\Users\admin1\Downloads\pd_v1.1_win\pd -p 784> lsass.dump
pd, version 1.1 tk 2006, [redacted]

Dump finished.

C:\>
```

12)



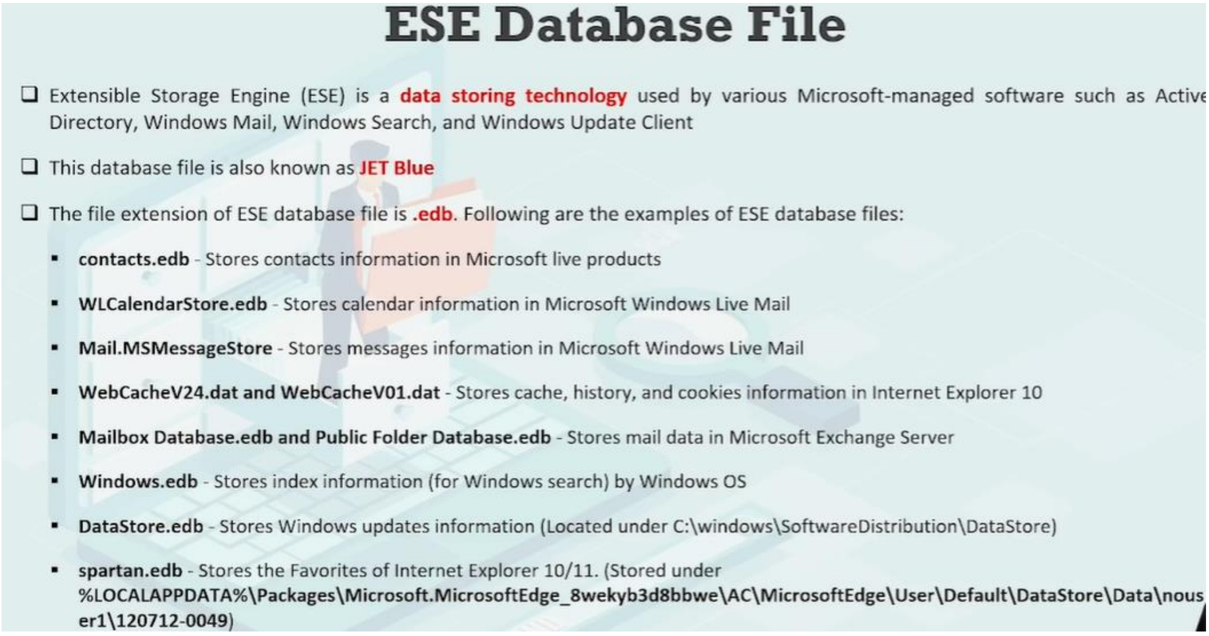
Collecting Network Status

- ❑ 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

Administrator: Command Prompt

```
C:\Windows\system32>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-NODV[redacted]
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Broadcom 802.11ac Network Adapter
   Physical Address. . . . . . . . . : A4-83-[redacted]-7D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e012:f149:5f48:2a81%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.102(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 17 April 2020 11:17:30
   Lease Expires . . . . . . . . . . : 18 April 2020 11:17:30
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 11144[redacted]7
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-1E-80-[redacted]-3C-7D
   DNS Servers . . . . . . . . . . . : 183.83.34.8
                                       123.176.37.36
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Windows\system32>
```

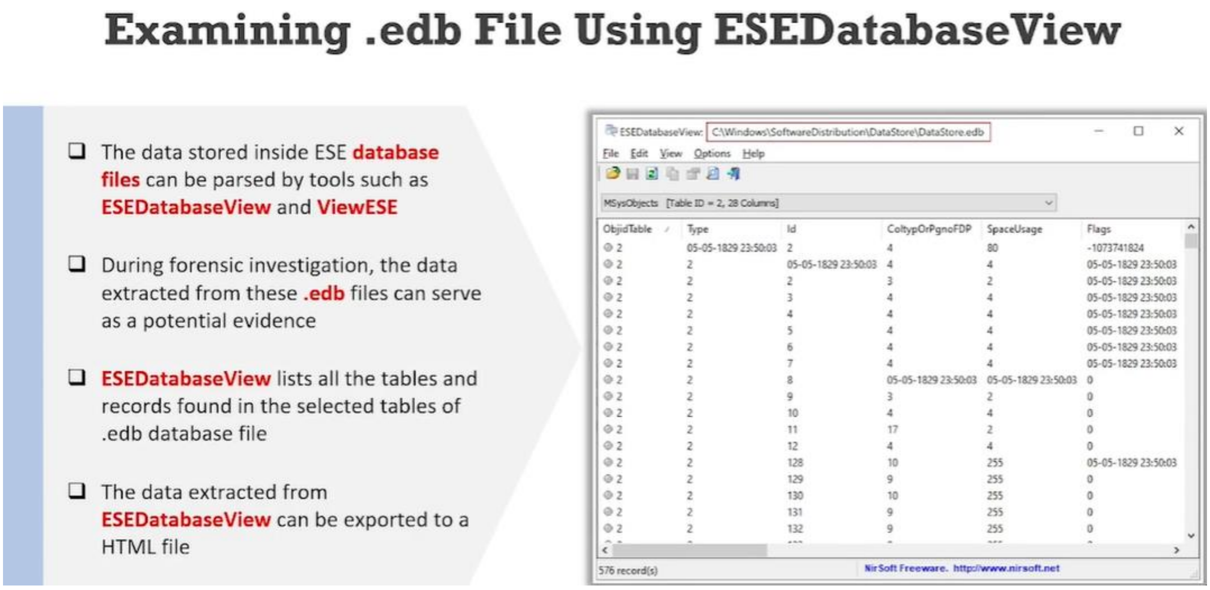
13)



ESE Database File

- ❑ Extensible Storage Engine (ESE) is a **data storing technology** used by various Microsoft-managed software such as Active Directory, Windows Mail, Windows Search, and Windows Update Client
- ❑ This database file is also known as **JET Blue**
- ❑ The file extension of ESE database file is **.edb**. Following are the examples of ESE database files:
  - ▪ **contacts.edb** - Stores contacts information in Microsoft live products
  - ▪ **WLCalendarStore.edb** - Stores calendar information in Microsoft Windows Live Mail
  - ▪ **Mail.MSMessageStore** - Stores messages information in Microsoft Windows Live Mail
  - ▪ **WebCacheV24.dat and WebCacheV01.dat** - Stores cache, history, and cookies information in Internet Explorer 10
  - ▪ **Mailbox Database.edb and Public Folder Database.edb** - Stores mail data in Microsoft Exchange Server
  - ▪ **Windows.edb** - Stores index information (for Windows search) by Windows OS
  - ▪ **DataStore.edb** - Stores Windows updates information (Located under C:\windows\SoftwareDistribution\DataStore)
  - ▪ **spartan.edb** - Stores the Favorites of Internet Explorer 10/11. (Stored under **%LOCALAPPDATA%\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\120712-0049**)

14)



Examining .edb File Using ESEDatabaseView

- ❑ The data stored inside ESE **database files** can be parsed by tools such as **ESEDatabaseView** and **ViewESE**
- ❑ During forensic investigation, the data extracted from these **.edb** files can serve as a potential evidence
- ❑ **ESEDatabaseView** lists all the tables and records found in the selected tables of .edb database file
- ❑ The data extracted from **ESEDatabaseView** can be exported to a HTML file

ESEDatabaseView: C:\Windows\SoftwareDistribution\DataStore\DataStore.edb

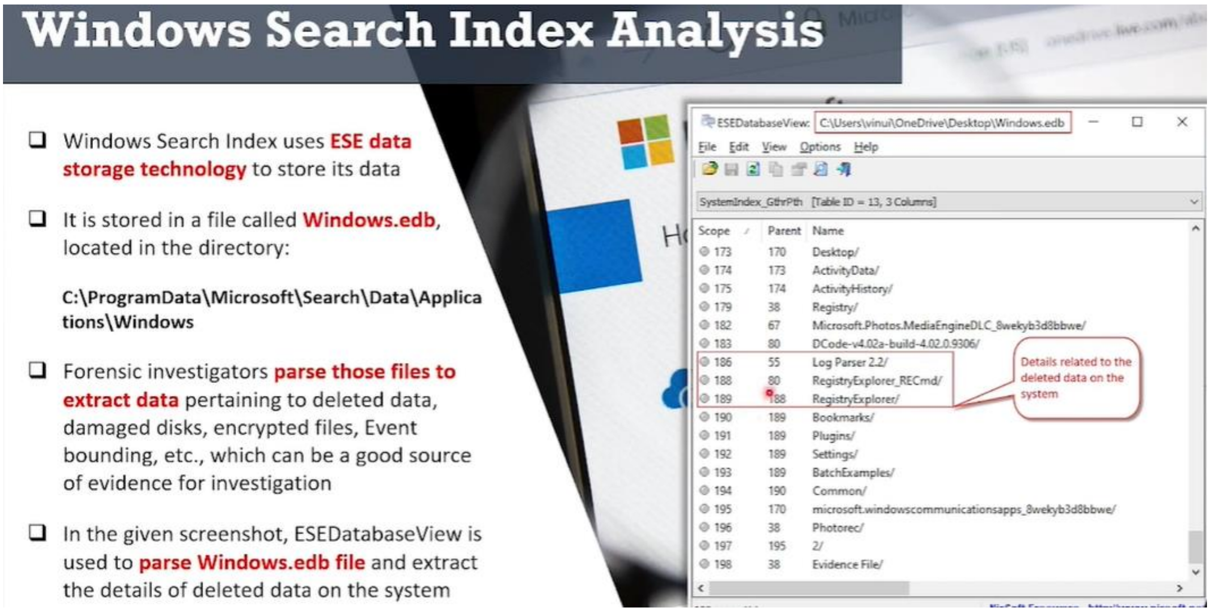
MSysObjects [Table ID = 2, 28 Columns]

ObjidTable	Type	Id	ColtypOrPgnoFDP	SpaceUsage	Flags
2	05-05-1829 23:50:03	2	4	80	-1073741824
2	2	05-05-1829 23:50:03	4	4	05-05-1829 23:50:03
2	2	2	3	2	05-05-1829 23:50:03
2	2	3	4	4	05-05-1829 23:50:03
2	2	4	4	4	05-05-1829 23:50:03
2	2	5	4	4	05-05-1829 23:50:03
2	2	6	4	4	05-05-1829 23:50:03
2	2	7	4	4	05-05-1829 23:50:03
2	2	8	05-05-1829 23:50:03	05-05-1829 23:50:03	0
2	2	9	3	2	0
2	2	10	4	4	0
2	2	11	17	2	0
2	2	12	4	4	0
2	2	128	10	255	05-05-1829 23:50:03
2	2	129	9	255	0
2	2	130	10	255	0
2	2	131	9	255	0
2	2	132	9	255	0

576 record(s)

NirSoft Freeware. http://www.nirsoft.net

15)



Windows Search Index Analysis

- ❑ Windows Search Index uses **ESE data storage technology** to store its data
- ❑ It is stored in a file called **Windows.edb**, located in the directory:

  C:\ProgramData\Microsoft\Search\Data\Applications\Windows
- ❑ Forensic investigators **parse those files to extract data** pertaining to deleted data, damaged disks, encrypted files, Event bounding, etc., which can be a good source of evidence for investigation
- ❑ In the given screenshot, ESEDatabaseView is used to **parse Windows.edb file** and extract the details of deleted data on the system

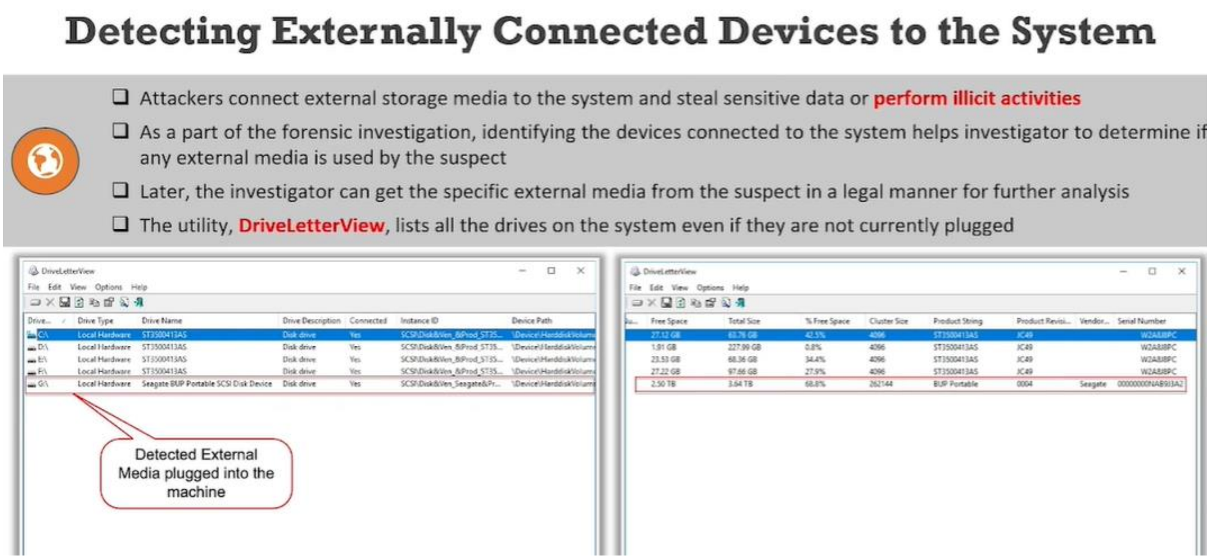
ESEDatabaseView: C:\Users\vinui\OneDrive\Desktop\Windows.edb

SystemIndex_GthrPth [Table ID = 13, 3 Columns]

Scope	Parent	Name
173	170	Desktop/
174	173	ActivityData/
175	174	ActivityHistory/
179	38	Registry/
182	67	Microsoft.Photos.MediaEngineDLC_8wekyb3d8bbwe/
183	80	DCode-v4.02a-build-4.02.0.9306/
186	55	Log Parser 2.2/
188	80	RegistryExplorer_RECmd/
189	188	RegistryExplorer/
190	189	Bookmarks/
191	189	Plugins/
192	189	Settings/
193	189	BatchExamples/
194	190	Common/
195	170	microsoft.windowscommunicationsapps_8wekyb3d8bbwe/
196	38	Photorec/
197	195	2/
198	38	Evidence File/

Details related to the deleted data on the system

17)



Detecting Externally Connected Devices to the System

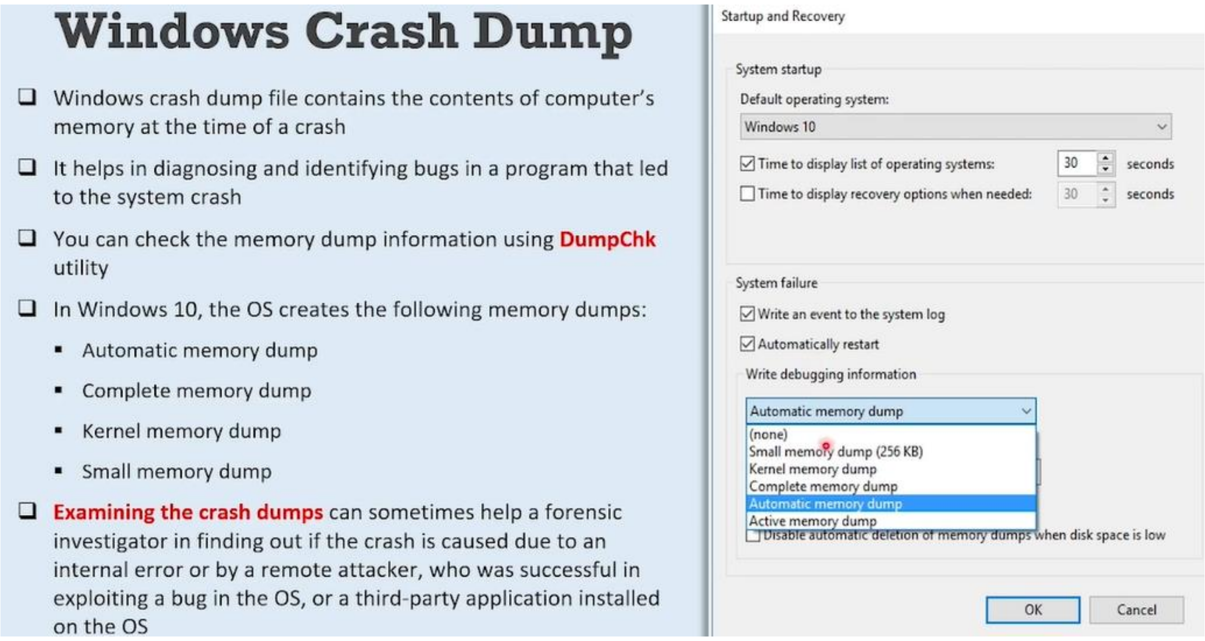
- ☐ Attackers connect external storage media to the system and steal sensitive data or **perform illicit activities**
- ☐ As a part of the forensic investigation, identifying the devices connected to the system helps investigator to determine if any external media is used by the suspect
- ☐ Later, the investigator can get the specific external media from the suspect in a legal manner for further analysis
- ☐ The utility, **DriveLetterView**, lists all the drives on the system even if they are not currently plugged

Drive...	Drive Type	Drive Name	Drive Description	Connected	Instance ID	Device Path
C:\	Local Hardware	ST3500413AS	Disk drive	Yes	SCSI\Disk&Ven_&Prod_ST35...	\Device\HarddiskVolum
D:\	Local Hardware	ST3500413AS	Disk drive	Yes	SCSI\Disk&Ven_&Prod_ST35...	\Device\HarddiskVolum
E:\	Local Hardware	ST3500413AS	Disk drive	Yes	SCSI\Disk&Ven_&Prod_ST35...	\Device\HarddiskVolum
F:\	Local Hardware	ST3500413AS	Disk drive	Yes	SCSI\Disk&Ven_&Prod_ST35...	\Device\HarddiskVolum
G:\	Local Hardware	Seagate BUP Portable SCSI Disk Device	Disk drive	Yes	SCSI\Disk&Ven_Seagate&Pr...	\Device\HarddiskVolum

Detected External Media plugged into the machine

Free Space	Total Size	% Free Space	Cluster Size	Product String	Product Revisi...	Vendor...	Serial Number
27.12 GB	63.76 GB	42.5%	4096	ST3500413AS	JC49		W2A8J8PC
1.91 GB	227.99 GB	0.8%	4096	ST3500413AS	JC49		W2A8J8PC
23.53 GB	68.36 GB	34.4%	4096	ST3500413AS	JC49		W2A8J8PC
27.22 GB	97.66 GB	27.9%	4096	ST3500413AS	JC49		W2A8J8PC
2.50 TB	3.64 TB	68.8%	262144	BUP Portable	0004	Seagate	00000000NAB9J3A2

18)



Windows Crash Dump

- ☐ Windows crash dump file contains the contents of computer's memory at the time of a crash
- ☐ It helps in diagnosing and identifying bugs in a program that led to the system crash
- ☐ 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
- ☐ **Examining the crash dumps** can sometimes help a forensic investigator in finding out if the crash is caused due to an internal error or by a remote attacker, who was successful in exploiting a bug in the OS, or a third-party application installed on the OS

Startup and Recovery

System startup

Default operating system: Windows 10

☑ Time to display list of operating systems: 30 seconds

☐ Time to display recovery options when needed: 30 seconds

System failure

☑ Write an event to the system log

☑ Automatically restart

Write debugging information

Automatic memory dump

☐ Disable automatic deletion of memory dumps when disk space is low

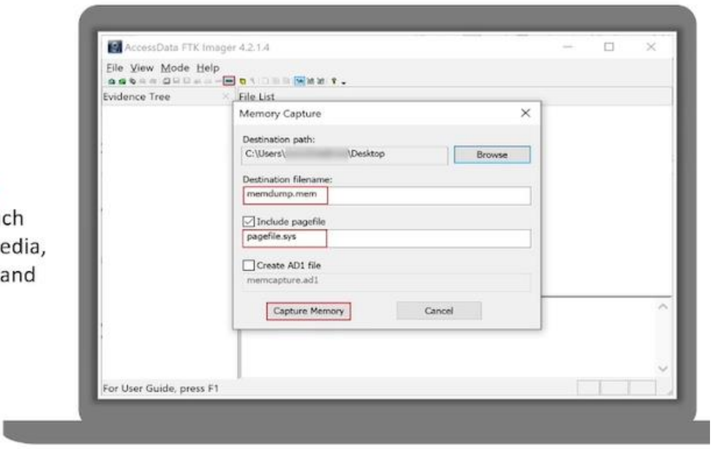
19)

Random Access Memory (RAM) Acquisition

01 Examining **volatile memory** is as important as non-volatile memory

02 From forensics point of view, **examining RAM dumps** provides system artifacts such as running services, accessed files and media, system processes, network information, and malware activity

03 During **live acquisition**, investigators use tools such as **Belkasoft RAM Capturer** and **AccessData FTK Imager** to perform RAM dumps



Destination path: C:\Users\[redacted]\Desktop

Destination filename: memdump.mem

☑ Include pagefile

pagefile.sys

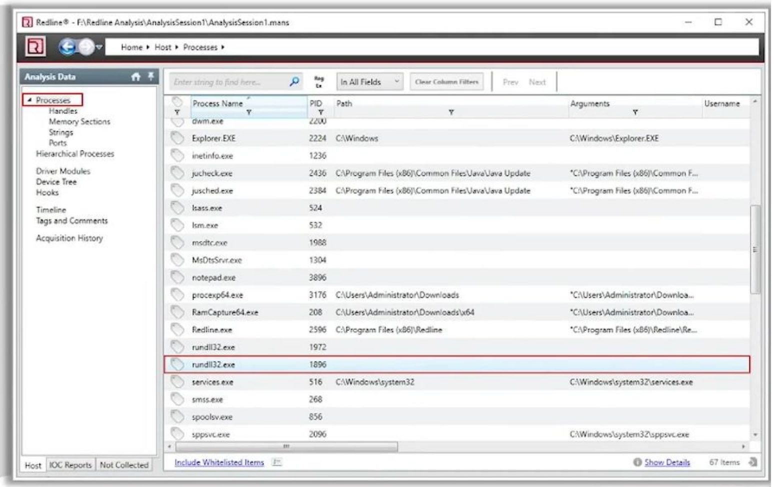
☐ Create AD1 file

memcapture.ad1

20)

Memory Forensics: Malware Analysis Using Redline

- ❑ Redline is a security tool to identify malicious activities through memory and helps forensic investigators to establish the **timeline and scope of an incident**
- ❑ Analyze the RAM dump using Redline by loading it from '**Analyze Data**' section
- ❑ Under '**Analysis Data**' tab, you can find all the processes running on the system when the RAM dump was acquired



Process Name	PID	Path	Arguments	Username
dwm.exe	2200			
Explorer.EXE	2224	C:\Windows	C:\Windows\Explorer.EXE	
inetinfo.exe	1236			
jucheck.exe	2436	C:\Program Files (x86)\Common Files\Java\Java Update	"C:\Program Files (x86)\Common F...	
jusched.exe	2384	C:\Program Files (x86)\Common Files\Java\Java Update	"C:\Program Files (x86)\Common F...	
lsass.exe	524			
lsm.exe	532			
msdtc.exe	1988			
MsDtsSrvr.exe	1304			
notepad.exe	3896			
procexp64.exe	3176	C:\Users\Administrator\Downloads	"C:\Users\Administrator\Downloa...	
RamCapture64.exe	208	C:\Users\Administrator\Downloads\x64	"C:\Users\Administrator\Downloa...	
Redline.exe	2596	C:\Program Files (x86)\Redline	"C:\Program Files (x86)\Redline\Re...	
rundll32.exe	1972			
rundll32.exe	1896			
services.exe	516	C:\Windows\system32	C:\Windows\system32\services.exe	
smss.exe	268			
spoolsv.exe	856			
sppsvc.exe	2096		C:\Windows\system32\sppsvc.exe	

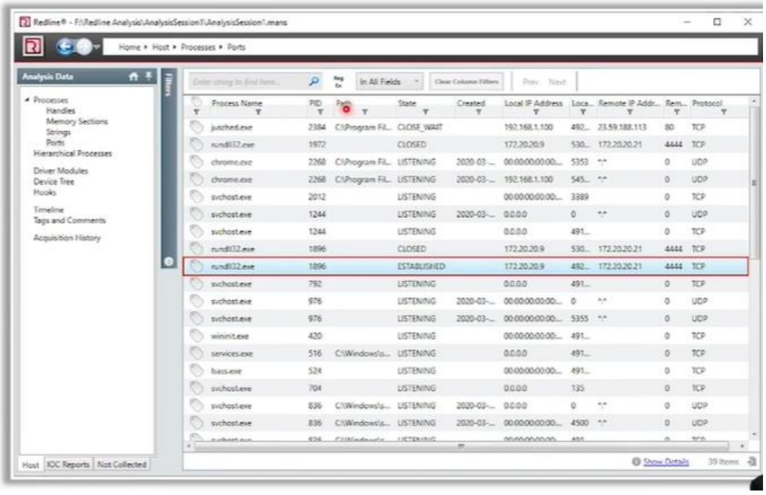
https://www.fireeye.co

21)

Memory Forensics: Malware Analysis Using Redline (Cont'd)

Click on '**Ports**' under '**Processes**' tab, where you can find all the connections available when the RAM dump was acquired

From the screenshot, it is observed that the Process '**rundll32.exe**', PID 1896 is making connection to Remote IP Address **172.20.20.21** over Port **4444**, which looks suspicious



Redline® - F:\Redline Analysis\AnalysisSession1\AnalysisSession1.mans

Home ▸ Host ▸ Processes ▸ Ports

Process Name	PID	Path	State	Created	Local IP Address	Loca...	Remote IP Addr...	Rem...	Protocol
jusched.exe	2384	C:\Program Fil...	CLOSE_WAIT		192.168.1.100	492...	23.59.188.113	80	TCP
rundll32.exe	1972		CLOSED		172.20.20.9	530...	172.20.20.21	4444	TCP
chrome.exe	2268	C:\Program Fil...	LISTENING	2020-03-...	00:00:00:00:00:...	5353	*:*	0	UDP
chrome.exe	2268	C:\Program Fil...	LISTENING	2020-03-...	192.168.1.100	545...	*:*	0	UDP
svchost.exe	2012		LISTENING		00:00:00:00:00:...	3389		0	TCP
svchost.exe	1244		LISTENING	2020-03-...	0.0.0.0	0	*:*	0	UDP
svchost.exe	1244		LISTENING		0.0.0.0	491...		0	TCP
rundll32.exe	1896		CLOSED		172.20.20.9	530...	172.20.20.21	4444	TCP
rundll32.exe	1896		ESTABLISHED		172.20.20.9	492...	172.20.20.21	4444	TCP
svchost.exe	792		LISTENING		0.0.0.0	491...		0	TCP
svchost.exe	976		LISTENING	2020-03-...	00:00:00:00:00:...	0	*:*	0	UDP
svchost.exe	976		LISTENING	2020-03-...	00:00:00:00:00:...	5355	*:*	0	UDP
wininit.exe	420		LISTENING		00:00:00:00:00:...	491...		0	TCP
services.exe	516	C:\Windows\s...	LISTENING		0.0.0.0	491...		0	TCP
lsass.exe	524		LISTENING		00:00:00:00:00:...	491...		0	TCP
svchost.exe	704		LISTENING		0.0.0.0	135		0	TCP
svchost.exe	836	C:\Windows\s...	LISTENING	2020-03-...	0.0.0.0	0	*:*	0	UDP
svchost.exe	836	C:\Windows\s...	LISTENING	2020-03-...	00:00:00:00:00:...	4500	*:*	0	UDP

22)

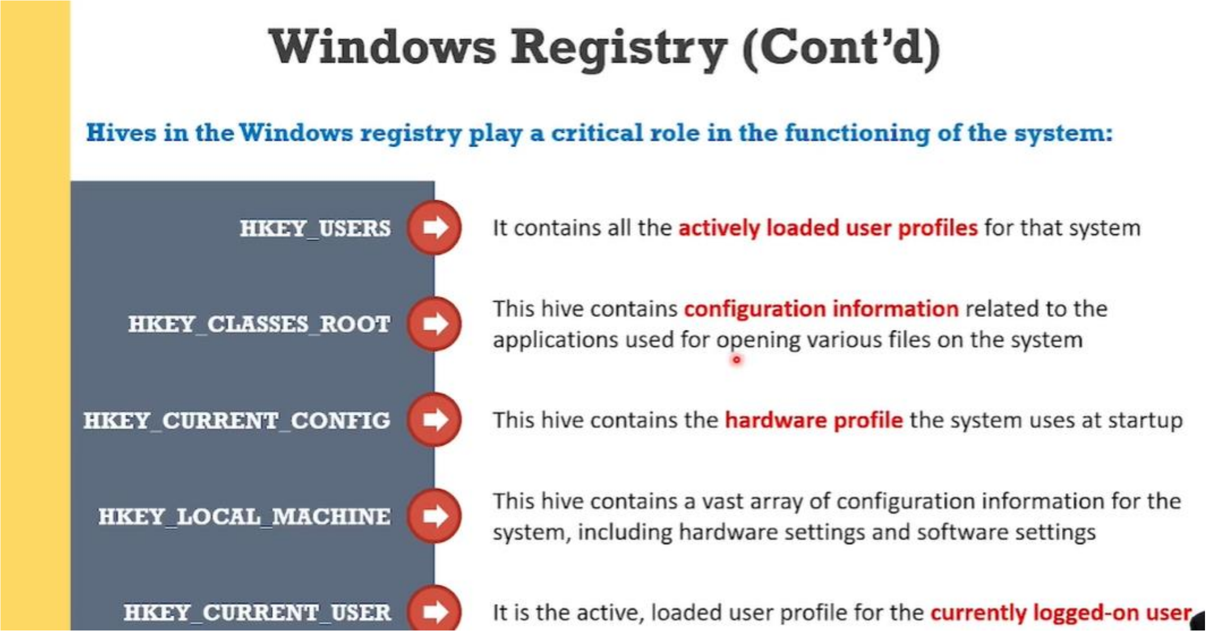
Windows Registry

- ❑ Every action performed by the user on the machine is **recorded in the Windows Registry**; Hence, it is a good source of evidence during forensic investigation
- ❑ With respect to data persistence, Windows Registry hives are divided into:

Non-volatile:	Volatile:
HKEY_LOCAL_MACHIN	HKEY_CLASSES_ROOT
HKEY_USERS	HKEY_CURRENT_USER
	HKEY_CURRENT_CONFIG

- ❑ The volatile hives are captured during **live analysis** of the system while the non-volatile hives are stored on the hard drive

23)

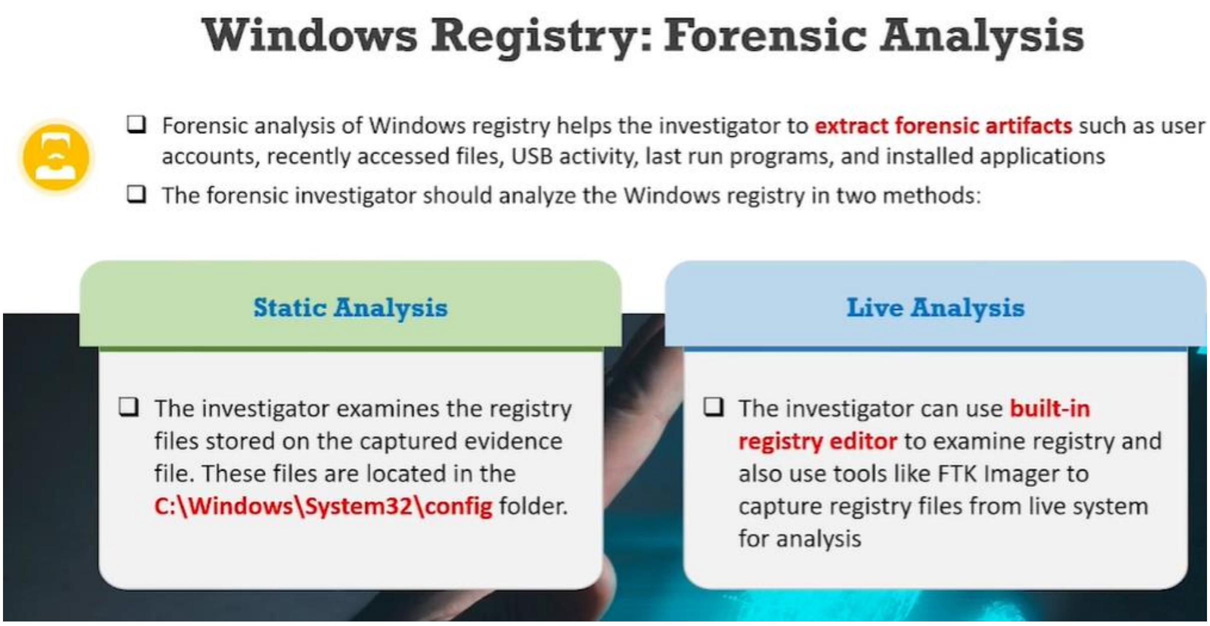


Windows Registry (Cont'd)

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

- **HKEY_USERS** ➡ It contains all the **actively loaded user profiles** for that system
- **HKEY_CLASSES_ROOT** ➡ This hive contains **configuration information** related to the applications used for opening various files on the system
- **HKEY_CURRENT_CONFIG** ➡ This hive contains the **hardware profile** the system uses at startup
- **HKEY_LOCAL_MACHINE** ➡ This hive contains a vast array of configuration information for the system, including hardware settings and software settings
- **HKEY_CURRENT_USER** ➡ It is the active, loaded user profile for the **currently logged-on user**

24)



Windows Registry: Forensic Analysis

❑ Forensic analysis of Windows registry helps the investigator to **extract forensic artifacts** such as user accounts, recently accessed files, USB activity, last run programs, and installed applications

❑ The forensic investigator should analyze the Windows registry in two methods:

Static Analysis

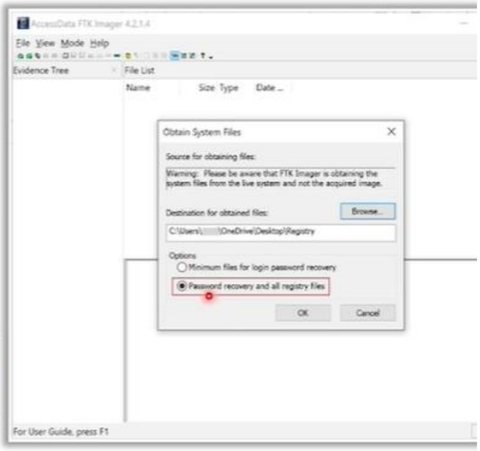
❑ The investigator examines the registry files stored on the captured evidence file. These files are located in the **C:\Windows\System32\config** folder.

Live Analysis

❑ The investigator can use **built-in registry editor** to examine registry and also use tools like FTK Imager to capture registry files from live system for analysis

Windows Registry: Forensic Analysis (Cont'd)

- ❑ To capture Windows registry files on Live system using FTK Imager:
  - Open FTK Imager and browse **File > Obtain Protected Files**
  - Select, **Password recovery and all registry files** (as shown in screenshot) and provide destination directory to extract the files



Obtain System Files

Source for obtaining files:

Warning: Please be aware that FTK Imager is obtaining the system files from the live system and not the acquired image.

Destination for obtained files: Browse...

C:\Users\[redacted]\OneDrive\Desktop\Registry

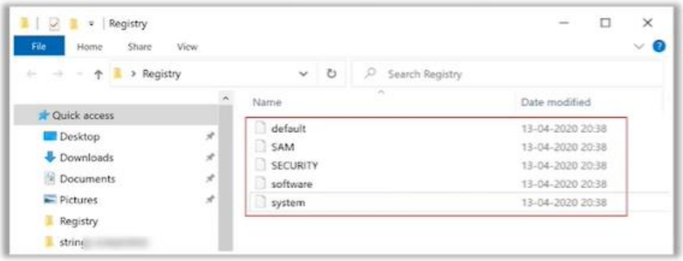
Options

○ Minimum files for login password recovery

● Password recovery and all registry files

OK Cancel

Sub Keys of HKEY_LOCAL_MACHINE Exported



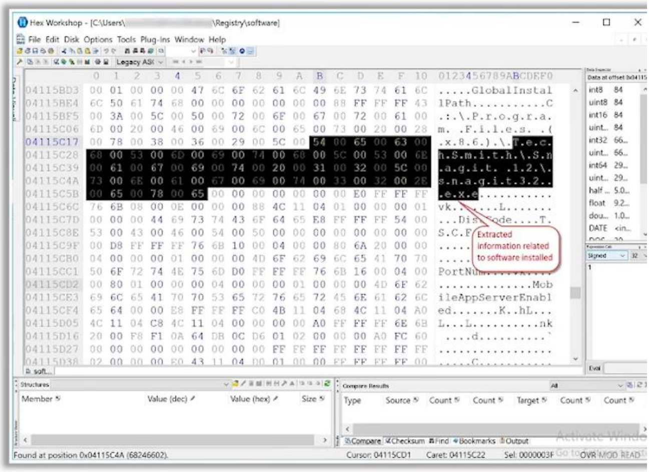
Name	Date modified
default	13-04-2020 20:38
SAM	13-04-2020 20:38
SECURITY	13-04-2020 20:38
software	13-04-2020 20:38
system	13-04-2020 20:38

25)

Windows Registry: Forensic Analysis (Cont'd)

- ❑ The extracted subkeys of **HKEY_LOCAL_MACHINE** contains following information:
  - **SAM (Security Account Manager)**: It is a local security database and subkeys in the SAM contains settings of user data and work groups
  - **Security**: It includes local security database in SAM
  - **Software**: It contains information about the software applications and their configuration settings on the system
  - **System**: It contains configuration settings of the hardware drivers and services
  - **Default**: It includes default user settings but **NTUSER.dat** file pertaining to the currently logged-on user overrides the default user settings

Forensic analysis of 'Software' subkey using Hex Editor



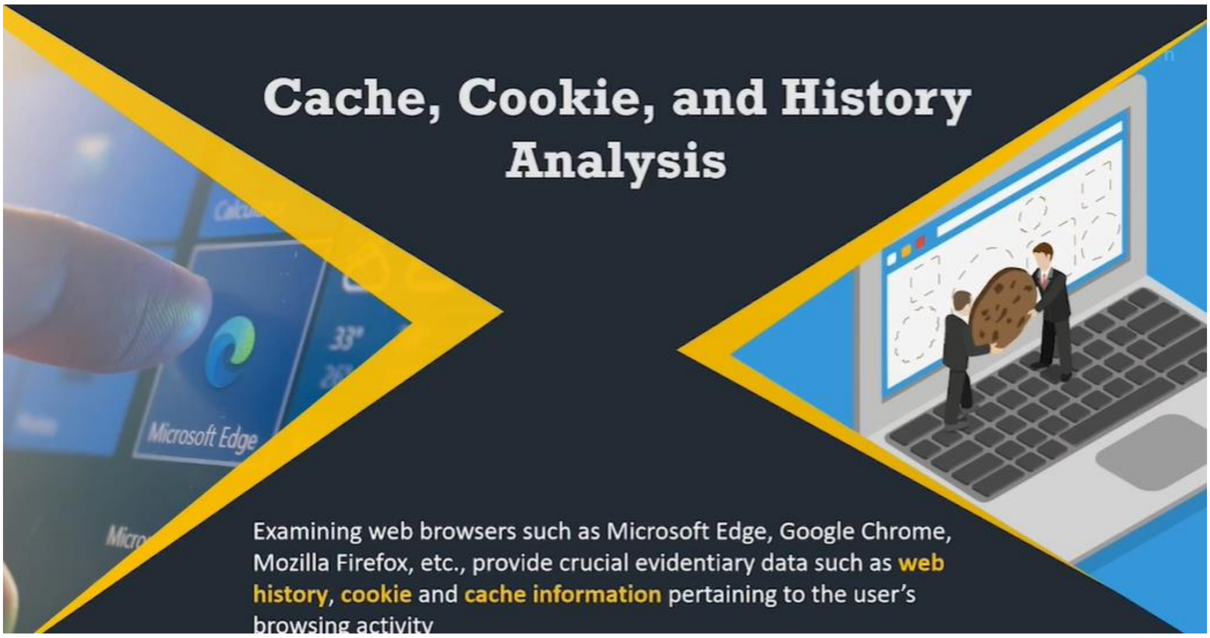
```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10  0123456789ABCDEF0
04115BD3 00 01 00 00 00 47 6C 6F 62 61 6C 49 6E 73 74 61 6C  .....GlobalInstal
04115BE4 6C 50 61 74 68 00 00 00 00 00 00 00 88 FF FF FF 43  lPath...........C
04115BF5 00 3A 00 5C 00 50 00 72 00 6F 00 67 00 72 00 61 00  .:.\.P.r.o.g.r.a.
04115C06 6D 00 20 00 46 00 69 00 6C 00 65 00 73 00 20 00 28  m. .F.i.l.e.s. .(
04115C17 00 78 00 38 00 36 00 29 00 5C 00 54 00 65 00 63 00  .x.8.6.).\.T.e.c.
04115C28 68 00 53 00 6D 00 69 00 74 00 68 00 5C 00 53 00 6E  h.S.m.i.t.h.\.S.n
04115C39 00 61 00 67 00 69 00 74 00 20 00 31 00 32 00 5C 00  .a.g.i.t. .1.2.\.
04115C4A 73 00 6E 00 61 00 67 00 69 00 74 00 33 00 32 00 2E  s.n.a.g.i.t.3.2..
04115C5B 00 65 00 78 00 65 00 00 00 00 00 00 00 E0 FF FF FF  .e.x.e...........
04115C6C 76 6B 08 00 0E 00 00 00 88 4C 11 04 01 00 00 00 01  vk.......L.......
04115C7D 00 00 00 44 69 73 74 43 6F 64 65 E8 FF FF FF 54 00  ...DistCode....T.
04115C8E 53 00 43 00 46 00 54 00 50 00 00 00 00 00 00 00 00  S.C.F
04115C9F 00 D8 FF FF FF 76 6B 10 00 04 00 00 80 6A 20 00 00  .....
04115CB0 04 00 00 00 01 00 00 00 4D 6F 62 69 6C 65 41 70 70  .....
04115CC1 50 6F 72 74 4E 75 6D D0 FF FF FF 76 6B 16 00 04 00  PortNum
04115CD2 00 80 01 00 00 00 04 00 00 00 01 00 00 00 4D 6F 62  ..............Mob
04115CE3 69 6C 65 41 70 70 53 65 72 76 65 72 45 6E 61 62 6C  ileAppServerEnabl
04115CF4 65 64 00 00 E8 FF FF FF C0 4B 11 04 68 4C 11 04 A0  ed.......K..hL...
04115D05 4C 11 04 C8 4C 11 04 00 00 00 00 A0 FF FF FF 6E 6B  L...L..........nk
04115D16 20 00 F8 F1 0A 64 DB 0C D6 01 02 00 00 00 A0 FC 60   ....d..........`
04115D27 00 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF  .................
04115D38 02 00 00 00 E0 43 11 04 D0 01 00 00 FF FF FF FF 00  .....C...........
```

Extracted information related to software installed

Found at position 0x04115C4A (68246602).   Cursor: 04115CD1   Caret: 04115C22   Sel: 0000003F

Note: The forensic investigator can examine these registry files using tools such as **Hex Workshop** to extract useful informatio

26)



Cache, Cookie, and History Analysis

Examining web browsers such as Microsoft Edge, Google Chrome, Mozilla Firefox, etc., provide crucial evidentiary data such as **web history**, **cookie** and **cache information** pertaining to the user's browsing activity

27)

Cache, Cookie, and History Analysis: Google Chrome

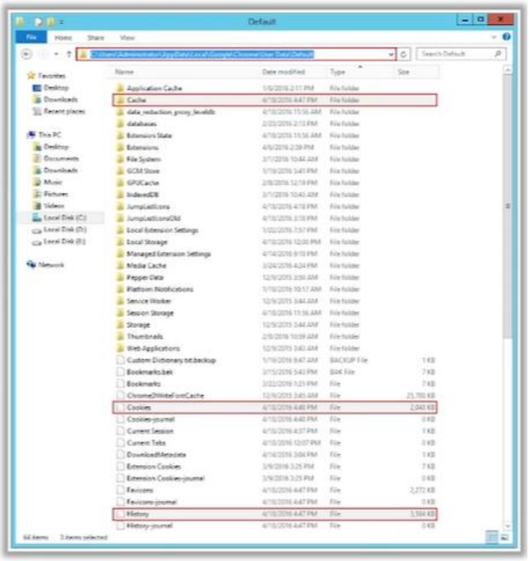
Google Chrome - Cache, cookies, and history are stored in the following system locations:

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



C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default

Name	Date modified	Type	Size
Application Cache	1/6/2016 2:11 PM	File folder	
Cache	4/18/2016 4:47 PM	File folder	
data_reduction_proxy_leveldb	4/18/2016 11:56 AM	File folder	
databases	2/23/2016 2:13 PM	File folder	
Extension State	4/18/2016 11:56 AM	File folder	
Extensions	4/6/2016 2:38 PM	File folder	
File System	3/1/2016 10:44 AM	File folder	
GCM Store	1/19/2016 3:41 PM	File folder	
GPUCache	2/8/2016 12:19 PM	File folder	
IndexedDB	3/1/2016 10:42 AM	File folder	
JumpListIcons	4/18/2016 4:18 PM	File folder	
JumpListIconsOld	4/18/2016 3:18 PM	File folder	
Local Extension Settings	1/22/2016 7:57 PM	File folder	
Local Storage	4/18/2016 12:00 PM	File folder	
Managed Extension Settings	4/14/2016 9:10 PM	File folder	
Media Cache	3/24/2016 4:24 PM	File folder	
Pepper Data	12/9/2015 3:50 AM	File folder	
Platform Notifications	1/18/2016 10:17 AM	File folder	
Service Worker	12/9/2015 3:44 AM	File folder	
Session Storage	4/18/2016 11:56 AM	File folder	
Storage	12/9/2015 3:44 AM	File folder	
Thumbnails	2/8/2016 10:59 AM	File folder	
Web Applications	12/9/2015 3:43 AM	File folder	
Custom Dictionary.txt.backup	1/19/2016 9:47 AM	BACKUP File	1 KB
Bookmarks.bak	3/15/2016 5:43 PM	BAK File	7 KB
Bookmarks	3/22/2016 1:21 PM	File	7 KB
ChromeDWriteFontCache	12/9/2015 3:45 AM	File	25,700 KB
Cookies	4/18/2016 4:48 PM	File	2,040 KB
Cookies-journal	4/18/2016 4:48 PM	File	0 KB
Current Session	4/18/2016 4:37 PM	File	1 KB
Current Tabs	4/18/2016 12:07 PM	File	0 KB
DownloadMetadata	4/14/2016 3:04 PM	File	1 KB
Extension Cookies	3/9/2016 3:25 PM	File	7 KB
Extension Cookies-journal	3/9/2016 3:25 PM	File	0 KB
Favicons	4/18/2016 4:47 PM	File	2,272 KB
Favicons-journal	4/18/2016 4:47 PM	File	0 KB
History	4/18/2016 4:47 PM	File	3,504 KB
History-journal	4/18/2016 4:47 PM	File	0 KB

64 items 3 items selected

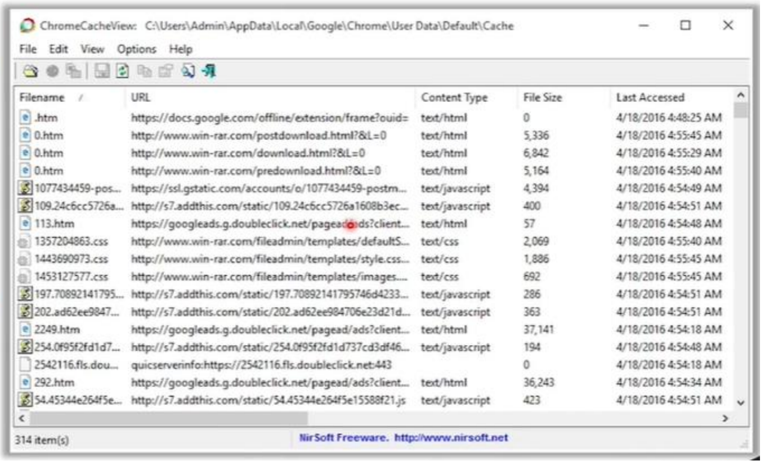
Analysis Tool: ChromeCacheView

1

ChromeCacheView is a **small utility** that reads the **cache folder** of Google Chrome and displays the list of all files currently stored in the cache

2

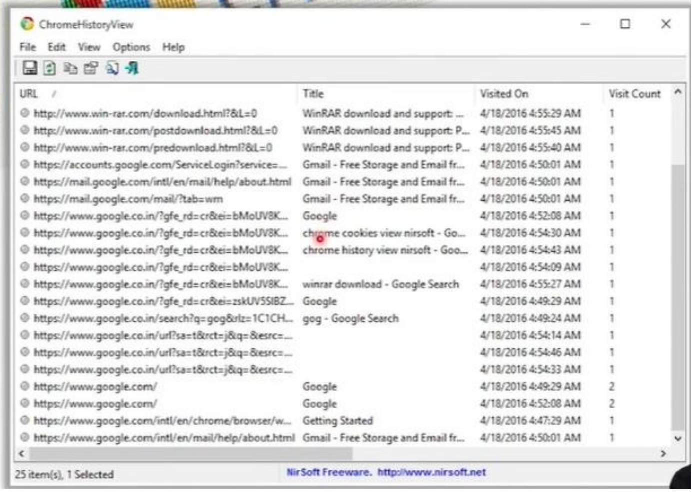
It displays the information such as **URL**, **Content Type**, **File Size**, **Last Accessed Time**, **Expiration Time**, **Server Name**, and **Server Response**


ChromeCacheView: C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Cache
File Edit View Options Help

Filename /	URL	Content Type	File Size	Last Accessed
.htm	https://docs.google.com/offline/extension/frame?ouid=	text/html	0	4/18/2016 4:48:25 AM
0.htm	http://www.win-rar.com/postdownload.html?&L=0	text/html	5,336	4/18/2016 4:55:45 AM
0.htm	http://www.win-rar.com/download.html?&L=0	text/html	6,842	4/18/2016 4:55:29 AM
0.htm	http://www.win-rar.com/predownload.html?&L=0	text/html	5,164	4/18/2016 4:55:40 AM
1077434459-pos...	https://ssl.gstatic.com/accounts/o/1077434459-postm...	text/javascript	4,394	4/18/2016 4:54:49 AM
109.24c6cc5726a...	http://s7.addthis.com/static/109.24c6cc5726a1608b3ec...	text/javascript	400	4/18/2016 4:54:51 AM
113.htm	https://googleads.g.doubleclick.net/pagead/ads?client...	text/html	57	4/18/2016 4:54:48 AM
1357204863.css	http://www.win-rar.com/fileadmin/templates/defaultS...	text/css	2,069	4/18/2016 4:55:40 AM
1443690973.css	http://www.win-rar.com/fileadmin/templates/style.css...	text/css	1,886	4/18/2016 4:55:45 AM
1453127577.css	http://www.win-rar.com/fileadmin/templates/images....	text/css	692	4/18/2016 4:55:45 AM
197.70892141795...	http://s7.addthis.com/static/197.70892141795746d4233...	text/javascript	286	4/18/2016 4:54:51 AM
202.ad62ee9847...	http://s7.addthis.com/static/202.ad62ee984706e23d21d...	text/javascript	363	4/18/2016 4:54:51 AM
2249.htm	https://googleads.g.doubleclick.net/pagead/ads?client...	text/html	37,141	4/18/2016 4:54:18 AM
254.0f95f2fd1d7...	http://s7.addthis.com/static/254.0f95f2fd1d737cd3df46...	text/javascript	194	4/18/2016 4:54:48 AM
2542116.fls.dou...	quicserverinfo:https://2542116.fls.doubleclick.net:443		0	4/18/2016 4:54:18 AM
292.htm	https://googleads.g.doubleclick.net/pagead/ads?client...	text/html	36,243	4/18/2016 4:54:34 AM
54.45344e264f5e...	http://s7.addthis.com/static/54.45344e264f5e15588f21.js	text/javascript	423	4/18/2016 4:54:51 AM

314 item(s) NirSoft Freeware. http://www.nirsoft.net

Analysis Tool: ChromeCookiesView



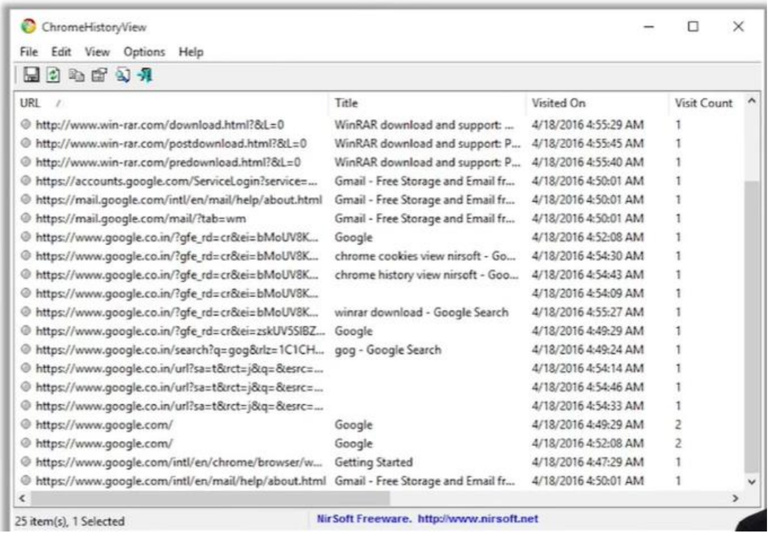
URL /	Title	Visited On	Visit Count
http://www.win-rar.com/download.html?&L=0	WinRAR download and support: ...	4/18/2016 4:55:29 AM	1
http://www.win-rar.com/postdownload.html?&L=0	WinRAR download and support: P...	4/18/2016 4:55:45 AM	1
http://www.win-rar.com/predownload.html?&L=0	WinRAR download and support: P...	4/18/2016 4:55:40 AM	1
https://accounts.google.com/ServiceLogin?service=...	Gmail - Free Storage and Email fr...	4/18/2016 4:50:01 AM	1
https://mail.google.com/intl/en/mail/help/about.html	Gmail - Free Storage and Email fr...	4/18/2016 4:50:01 AM	1
https://mail.google.com/mail/?tab=wm	Gmail - Free Storage and Email fr...	4/18/2016 4:50:01 AM	1
https://www.google.co.in/?gfe_rd=cr&ei=bMoUV8K...	Google	4/18/2016 4:52:08 AM	1
https://www.google.co.in/?gfe_rd=cr&ei=bMoUV8K...	chrome cookies view nirsoft - Go...	4/18/2016 4:54:30 AM	1
https://www.google.co.in/?gfe_rd=cr&ei=bMoUV8K...	chrome history view nirsoft - Goo...	4/18/2016 4:54:43 AM	1
https://www.google.co.in/?gfe_rd=cr&ei=bMoUV8K...		4/18/2016 4:54:09 AM	1
https://www.google.co.in/?gfe_rd=cr&ei=bMoUV8K...	winrar download - Google Search	4/18/2016 4:55:27 AM	1
https://www.google.co.in/?gfe_rd=cr&ei=zskUV5SIBZ...	Google	4/18/2016 4:49:29 AM	1
https://www.google.co.in/search?q=gog&rlz=1C1CH...	gog - Google Search	4/18/2016 4:49:24 AM	1
https://www.google.co.in/url?sa=t&rct=j&q=&esrc=...		4/18/2016 4:54:14 AM	1
https://www.google.co.in/url?sa=t&rct=j&q=&esrc=...		4/18/2016 4:54:46 AM	1
https://www.google.co.in/url?sa=t&rct=j&q=&esrc=...		4/18/2016 4:54:33 AM	1
https://www.google.com/	Google	4/18/2016 4:49:29 AM	2
https://www.google.com/	Google	4/18/2016 4:52:08 AM	2
https://www.google.com/intl/en/chrome/browser/w...	Getting Started	4/18/2016 4:47:29 AM	1
https://www.google.com/intl/en/mail/help/about.html	Gmail - Free Storage and Email fr...	4/18/2016 4:50:01 AM	1

25 item(s), 1 Selected NirSoft Freeware. http://www.nirsoft.net

- ❑ ChromeCookiesView displays the list of all **cookies** stored by Google Chrome, and allows investigators to export the cookies into a **text/CSV/html/XML file**
- ❑ It **displays information** such as Host Name, Path, Name, Value, Secure (Yes/No), HTTP Only Cookie (Yes/No), Last Accessed Time, Creation Time, and Expiration Time for each cookie

Analysis Tool: ChromeHistoryView

- ❑ ChromeHistoryView reads the **history data file** of Google Chrome and displays the list of all visited Web pages in the last days
- ❑ It displays **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



URL	Title	Visited On	Visit Count
http://www.win-rar.com/download.html?&L=0	WinRAR download and support: ...	4/18/2016 4:55:29 AM	1
http://www.win-rar.com/postdownload.html?&L=0	WinRAR download and support: P...	4/18/2016 4:55:45 AM	1
http://www.win-rar.com/predownload.html?&L=0	WinRAR download and support: P...	4/18/2016 4:55:40 AM	1
https://accounts.google.com/ServiceLogin?service=...	Gmail - Free Storage and Email fr...	4/18/2016 4:50:01 AM	1
https://mail.google.com/intl/en/mail/help/about.html	Gmail - Free Storage and Email fr...	4/18/2016 4:50:01 AM	1
https://mail.google.com/mail/?tab=wm	Gmail - Free Storage and Email fr...	4/18/2016 4:50:01 AM	1
https://www.google.co.in/?gfe_rd=cr&ei=bMoUV8K...	Google	4/18/2016 4:52:08 AM	1
https://www.google.co.in/?gfe_rd=cr&ei=bMoUV8K...	chrome cookies view nirsoft - Go...	4/18/2016 4:54:30 AM	1
https://www.google.co.in/?gfe_rd=cr&ei=bMoUV8K...	chrome history view nirsoft - Goo...	4/18/2016 4:54:43 AM	1
https://www.google.co.in/?gfe_rd=cr&ei=bMoUV8K...		4/18/2016 4:54:09 AM	1
https://www.google.co.in/?gfe_rd=cr&ei=bMoUV8K...	winrar download - Google Search	4/18/2016 4:55:27 AM	1
https://www.google.co.in/?gfe_rd=cr&ei=zskUV5SIBZ...	Google	4/18/2016 4:49:29 AM	1
https://www.google.co.in/search?q=gog&rlz=1C1CH...	gog - Google Search	4/18/2016 4:49:24 AM	1
https://www.google.co.in/url?sa=t&rct=j&q=&esrc=...		4/18/2016 4:54:14 AM	1
https://www.google.co.in/url?sa=t&rct=j&q=&esrc=...		4/18/2016 4:54:46 AM	1
https://www.google.co.in/url?sa=t&rct=j&q=&esrc=...		4/18/2016 4:54:33 AM	1
https://www.google.com/	Google	4/18/2016 4:49:29 AM	2
https://www.google.com/	Google	4/18/2016 4:52:08 AM	2
https://www.google.com/intl/en/chrome/browser/w...	Getting Started	4/18/2016 4:47:29 AM	1
https://www.google.com/intl/en/mail/help/about.html	Gmail - Free Storage and Email fr...	4/18/2016 4:50:01 AM	1

25 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

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

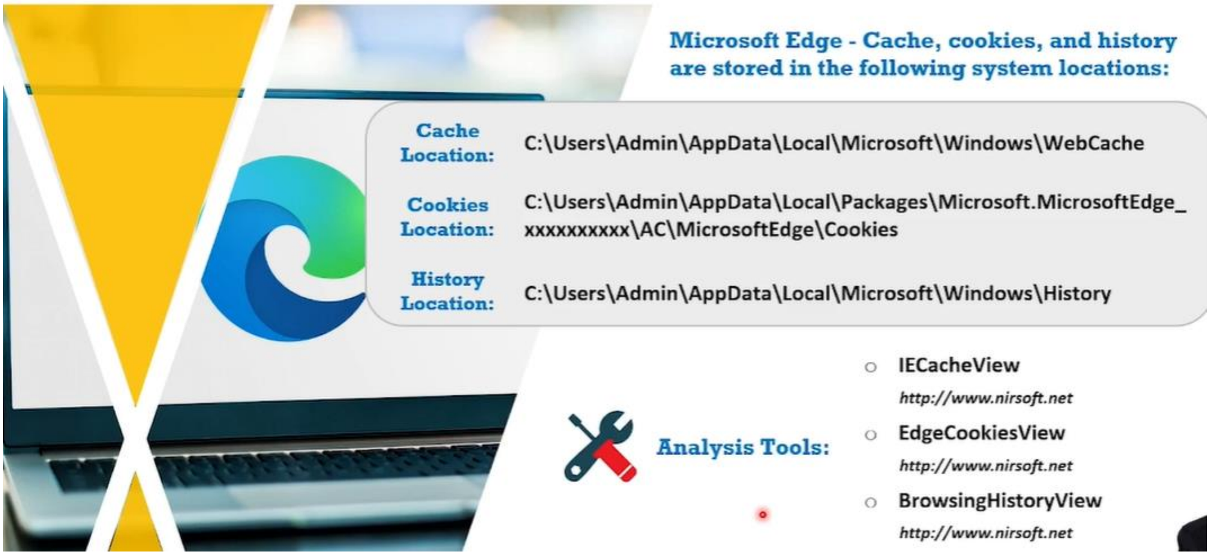
Cookies Location: C:\Users\<Username>\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\cookies.sqlite

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

Analysis Tools:

- ○ MZCacheView
  http://www.nirsoft.net
- ○ MZCookiesView
  https://www.zimperium.com
- ○ MZHistoryView
  http://www.nirsoft.net

Cache, Cookie, and History Analysis: Microsoft Edge



Microsoft Edge - Cache, cookies, and history are stored in the following system locations:

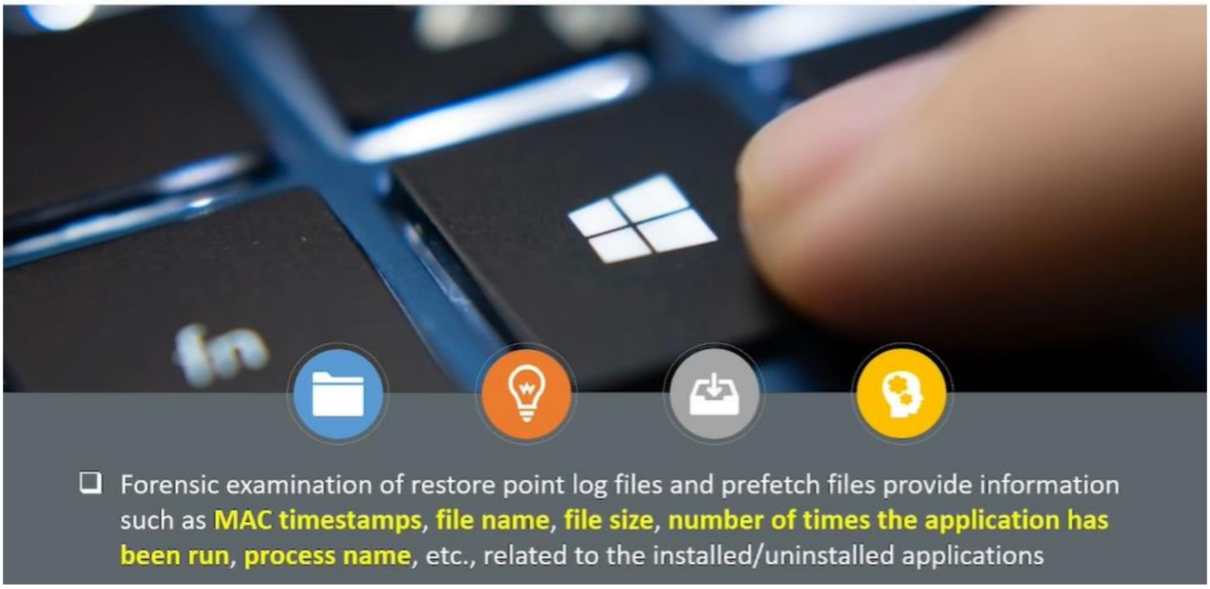
Cache Location:	C:\Users\Admin\AppData\Local\Microsoft\Windows\WebCache
Cookies Location:	C:\Users\Admin\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxxxxxxxx\AC\MicrosoftEdge\Cookies
History Location:	C:\Users\Admin\AppData\Local\Microsoft\Windows\History

Analysis Tools:

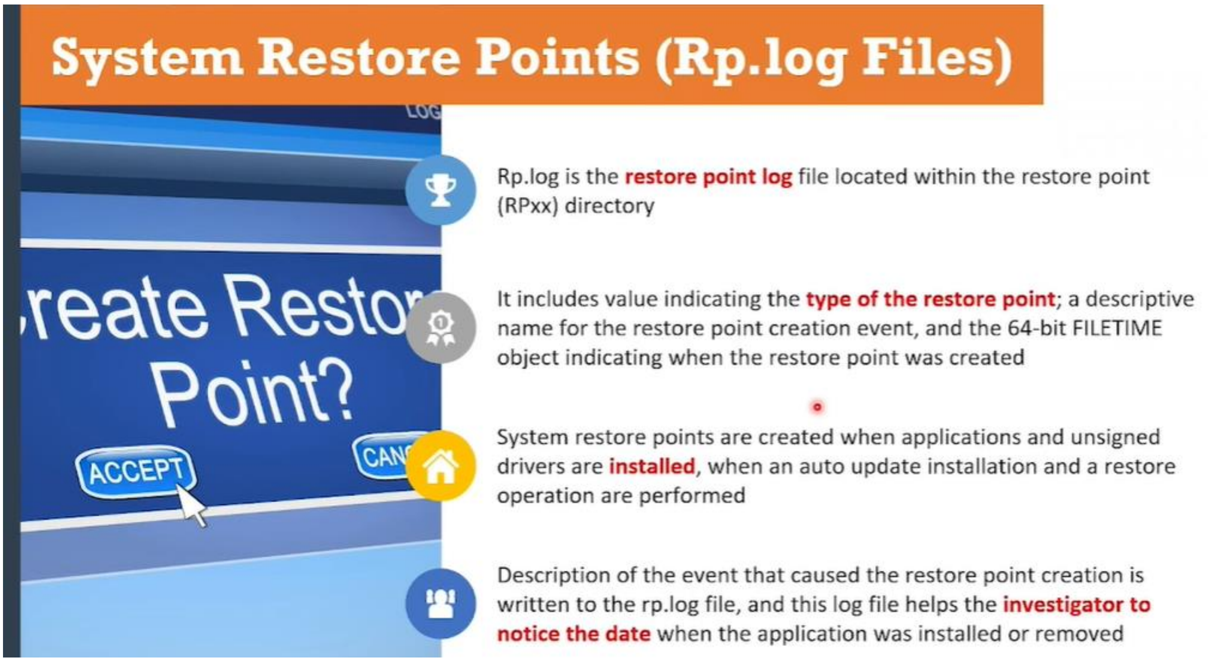
- ○ IECacheView *http://www.nirsoft.net*
- ○ EdgeCookiesView *http://www.nirsoft.net*
- ○ BrowsingHistoryView *http://www.nirsoft.net*

28)

Windows File Analysis

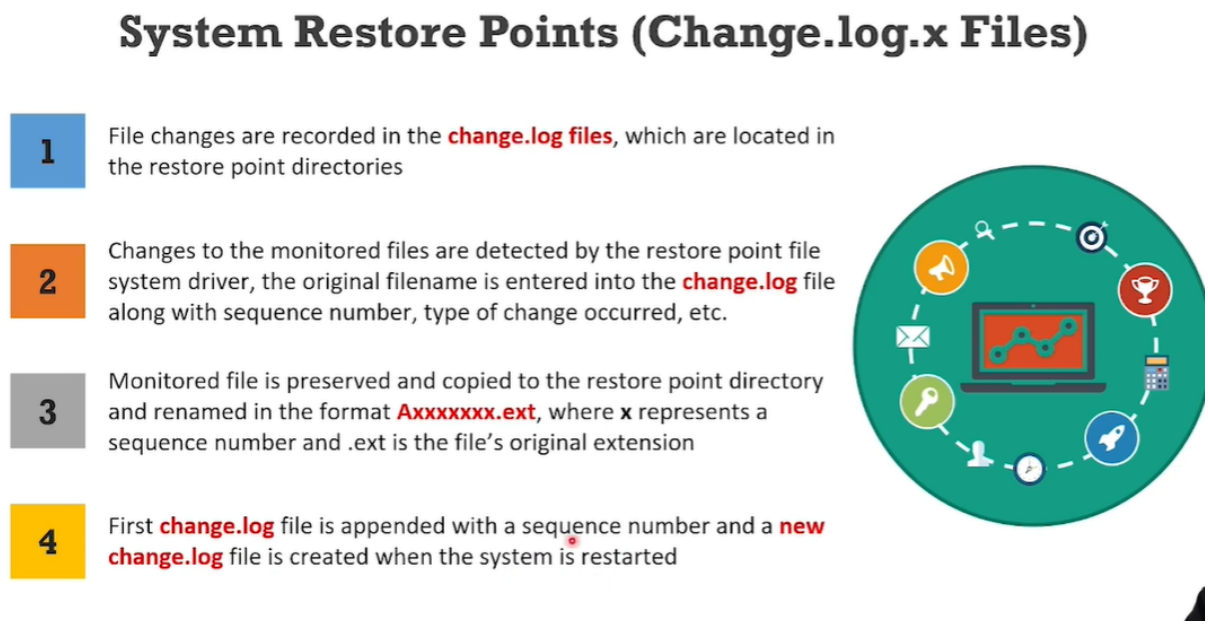


❑ Forensic examination of restore point log files and prefetch files provide information such as **MAC timestamps**, **file name**, **file size**, **number of times the application has been run**, **process name**, etc., related to the installed/uninstalled applications



System Restore Points (Rp.log Files)

- Rp.log is the **restore point log** file located within the restore point (RPxx) directory
- 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
- System restore points are created when applications and unsigned drivers are **installed**, when an auto update installation and a restore operation are performed
- Description of the event that caused the restore point creation is written to the rp.log file, and this log file helps the **investigator to notice the date** when the application was installed or removed



System Restore Points (Change.log.x Files)

1 File changes are recorded in the **change.log files**, which are located in the restore point directories

2 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.

3 Monitored file is preserved and copied to the restore point directory and renamed in the format **Axxxxxxx.ext**, where **x** represents a sequence number and .ext is the file's original extension

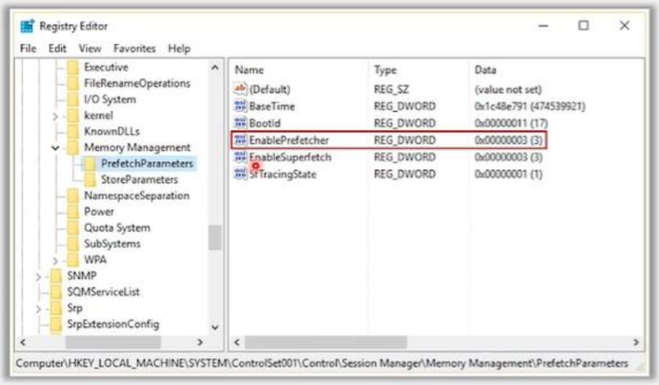
4 First **change.log** file is appended with a sequence number and a **new change.log** file is created when the system is restarted

Prefetch Files

1. When a user installs an application, runs it, and deletes it, traces of that application can be found in the **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.

Prefetch Files (Cont'd)

- ❑ Prefetching is used by the Windows OS to **speed up system boot process** and application launches
- ❑ The data is recorded for up to first 10 seconds after the application process is started
- ❑ Once the data is processed, it is written to a **.pf** file in the **Windows\Prefetch** directory
- ❑ The forensic investigator should identify whether the victim's system has enabled the prefetching process, before conducting examination



Name	Type	Data
(Default)	REG_SZ	(value not set)
BaseTime	REG_DWORD	0x1c48e791 (474539921)
BootId	REG_DWORD	0x00000011 (17)
EnablePrefetcher	REG_DWORD	0x00000003 (3)
EnableSuperfetch	REG_DWORD	0x00000003 (3)
SfTracingState	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\Memory Management\PrefetchParameters

- ❑ Prefetching is controlled by the registry key:

  `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00x\Control\SessionManager\MemoryManagement\PrefetchParameters`

- ❑ The data associated with value of **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

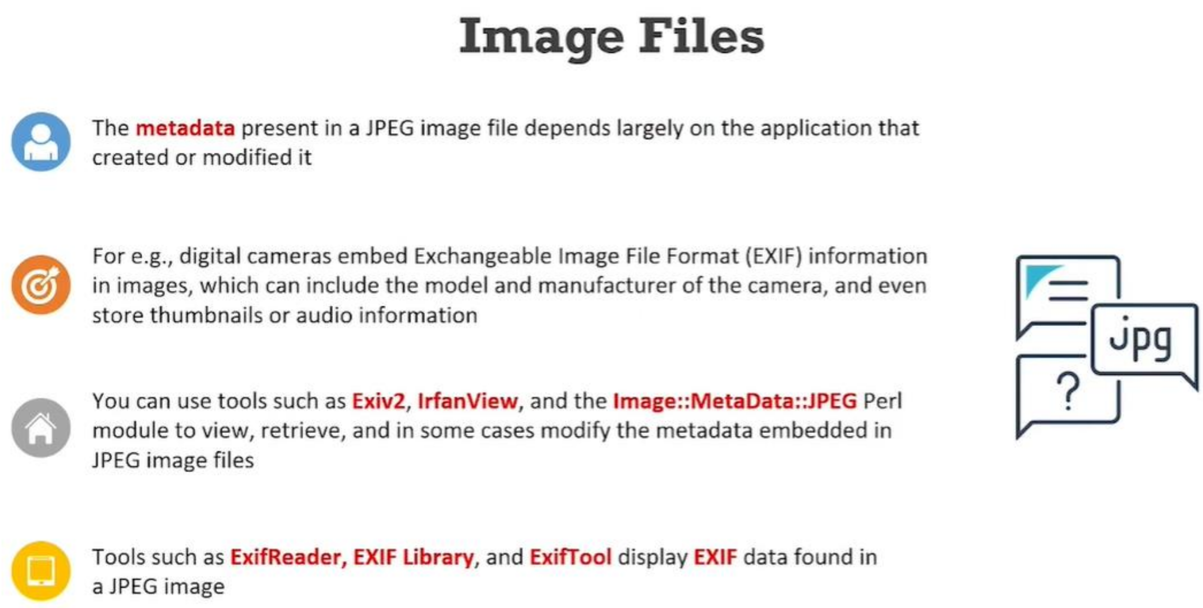
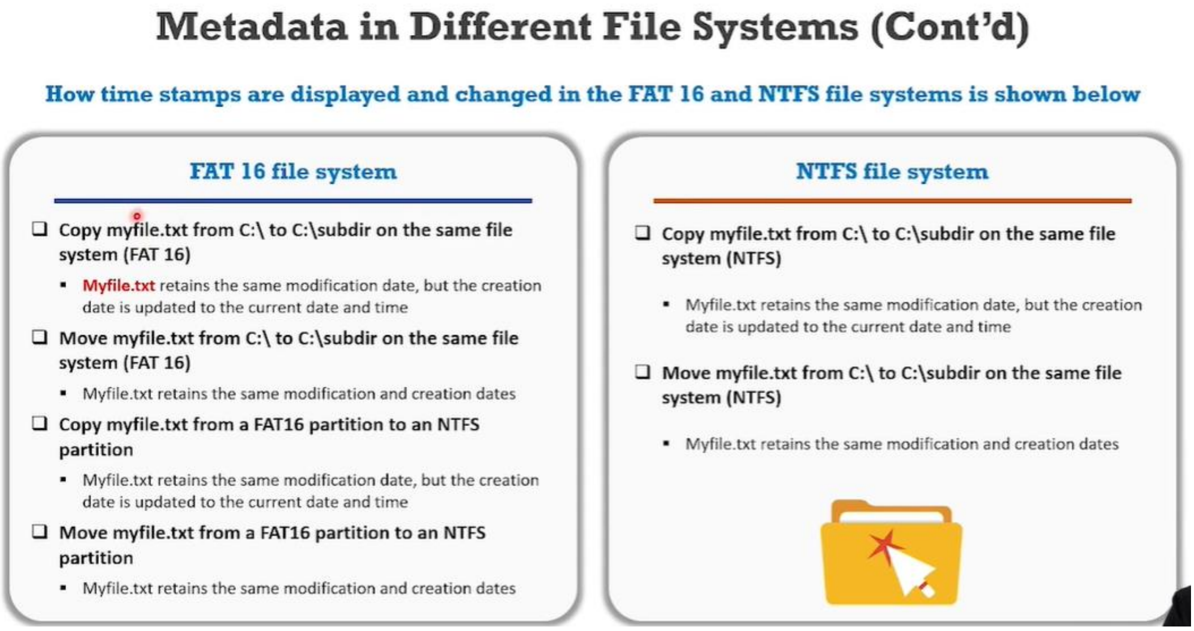


Image Files

- 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 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
- Tools such as **ExifReader, EXIF Library**, and **ExifTool** display **EXIF** data found in a JPEG image

29)



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

- ❑ Copy myfile.txt from C:\ to C:\subdir on the same file system (FAT 16)
  - **Myfile.txt** retains the same modification date, but the creation date is updated to the current date and time
- ❑ Move myfile.txt from C:\ to C:\subdir on the same file system (FAT 16)
  - Myfile.txt retains the same modification and creation dates
- ❑ Copy myfile.txt from a FAT16 partition to an NTFS partition
  - Myfile.txt retains 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 retains the same modification and creation dates

NTFS file system

- ❑ Copy myfile.txt from C:\ to C:\subdir on the same file system (NTFS)
  - Myfile.txt retains the same modification date, but the creation date is updated to the current date and time
- ❑ Move myfile.txt from C:\ to C:\subdir on the same file system (NTFS)
  - Myfile.txt retains the same modification and creation dates