

COMP 5350 / 6350

Digital Forensics

Windows Operating System Forensics



Exam Style Questions

How many bytes are in one sector of the hard drive shown below?

- a) 512 bytes
- b) 4096 bytes
- c) 32,728 bytes
- d) 65,536 bytes



ADVANCED
4Kn
FORMAT

How many bytes are in one sector of the hard drive shown below?

a) 512 bytes

b) 4096 bytes

c) 32,728 bytes

d) 65,536 bytes



ADVANCED
4Kn
FORMAT

The SD card shown below will be storing data files that will be approximately 3 GB each. Which of the following would be potential file systems that could support this file size?

- a) FAT12
- b) FAT16
- c) FAT32
- d) NTFS



The SD card shown below will be storing data files that will be approximately 3 GB each. Which of the following would be potential file systems that could support this file size?

a) FAT12

b) FAT16

c) FAT32

d) NTFS



Specify the name of each NTFS partition area shown below



Specify the name of each NTFS partition area shown below

a	b	c	d
---	---	---	---

**Master
Boot
Record**

**Master
File
Table**

**File
Data
Area**

**Master
File
Table
Backup**

For the NTFS MBR shown below, specify the correct value of the start of the MFT cluster:

- a) 0x00FF
- b) 0x003F
- c) 0xEB52
- d) 0xA6AA

Offset	00 01 02 03 04 05 06 07	08 09 0A 0B 0C 0D 0E 0F	ASCII
00100000	EB 52 90 4E 54 46 53 20	20 20 20 00 02 08 00 00	er.NTFS
00100010	00 00 00 00 00 F8 00 00	3F 00 FF 00 00 08 00 00	...0..?.ÿ....
00100020	00 00 00 00 80 00 00 00	FF 9F 0F 00 00 00 00 00	...ÿ.....
00100030	AA A6 00 00 00 00 00 00	02 00 00 00 00 00 00 00	a
00100040	F6 00 00 00 01 00 00 00	68 D7 81 F6 04 82 F6 E4	ö...h×.ö..öä
00100050	00 00 00 00 FA 33 C0 8E	D0 BC 00 7C FB 68 C0 07	...ú3Ä.Ð¼. ûhÄ.
00100060	1F 1E 68 66 00 CB 88 16	0E 00 66 81 3E 03 00 4E	..hf.Ë....f.>..N

NTFS Boot Sector		
Description	Offset	Bytes
Bootstrap Jump Command	0000h	3
OEM Identification	0003h	8
Bytes / Sector	000Bh	2
Sectors / Cluster	000Dh	1
Reserved Sectors	000Eh	2
Always 0	0010h	3
Not Used By NTFS	0013h	2
Media Descriptor	0015h	1
Always 0	0016h	2
Sectors / Track	0018h	2
Number of Heads	001Ah	2
Hidden Sectors	001Ch	4
Not Used By NTFS	0020h	4
Not Used By NTFS	0024h	4
Total Sectors	0028h	8
\$MFT Cluster Number	0030h	8
\$MFTMirr Cluster Number	0038h	8
Clusters / File Record	0040h	4
Clusters / Index Buffer	0044h	1
Not Used By NTFS	0045h	3
Volume Serial Number	0048h	8
Checksum	0050h	4
Bootstrap Code	003Eh	426
Boot Sector Signature	01FEh	2

For the NTFS MBR shown below, specify the correct value of the start of the MFT cluster:

a) 0x00FF

b) 0x003F

c) 0xEB52

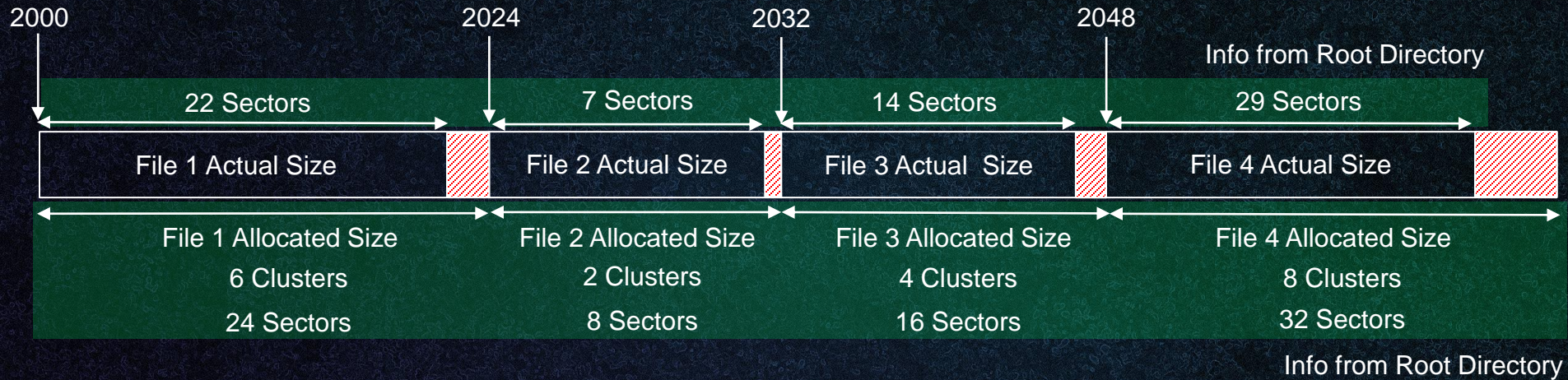
d) 0xA6AA

Offset	00 01 02 03 04 05 06 07	08 09 0A 0B 0C 0D 0E 0F	ASCII
00100000	EB 52 90 4E 54 46 53 20	20 20 20 00 02 08 00 00	NTFS
00100010	00 00 00 00 00 F8 00 00	3F 00 FF 00 00 08 00 00	...
00100020	00 00 00 00 80 00 00 00	FF 9F 0F 00 00 00 00 00	...
00100030	AA A6 00 00 00 00 00 00	02 00 00 00 00 00 00 00	a
00100040	F6 00 00 00 01 00 00 00	68 D7 81 F6 04 82 F6 E4	ö...h×.ö..öä
00100050	00 00 00 00 FA 33 C0 8E	D0 BC 00 7C FB 68 C0 07	...ú3Ä.Ð¼. ûhÄ.
00100060	1F 1E 68 66 00 CB 88 16	0E 00 66 81 3E 03 00 4E	..hf.Ë....f.>..N

NTFS Boot Sector		
Description	Offset	Bytes
Bootstrap Jump Command	0000h	3
OEM Identification	0003h	8
Bytes / Sector	000Bh	2
Sectors / Cluster	000Dh	1
Reserved Sectors	000Eh	2
Always 0	0010h	3
Not Used By NTFS	0013h	2
Media Descriptor	0015h	1
Always 0	0016h	2
Sectors / Track	0018h	2
Number of Heads	001Ah	2
Hidden Sectors	001Ch	4
Not Used By NTFS	0020h	4
Not Used By NTFS	0024h	4
Total Sectors	0028h	8
\$MFT Cluster Number	0030h	8
\$MFTMirr Cluster Number	0038h	8
Clusters / File Record	0040h	4
Clusters / Index Buffer	0044h	1
Not Used By NTFS	0045h	3
Volume Serial Number	0048h	8
Checksum	0050h	4
Bootstrap Code	003Eh	426
Boot Sector Signature	01FEh	2

FAT16 Deleted File Recovery

FAT16 Data Area Contents



File 1 – Skip (-s) 2000 – # Sectors (-n) 22
File 2 – Skip (-s) 2024 – # Sectors (-n) 7
File 3 – Skip (-s) 2032 – # Sectors (-n) 14
File 4 – Skip (-s) 2048 – # Sectors (-n) 29



* 4 Sectors / Cluster

Windows VM Configuration

Windows 10 Education

- We will utilize an education version of Windows 10 to conduct forensic analysis of Windows artifacts
- Student Windows 10 Version
 - ✓ <https://azureforeducation.microsoft.com/devtools>

The screenshot shows the Microsoft Azure Education Software page. The search bar contains 'windows 10'. The results show 32 items. The table below lists the first four items, with the last item highlighted in red.

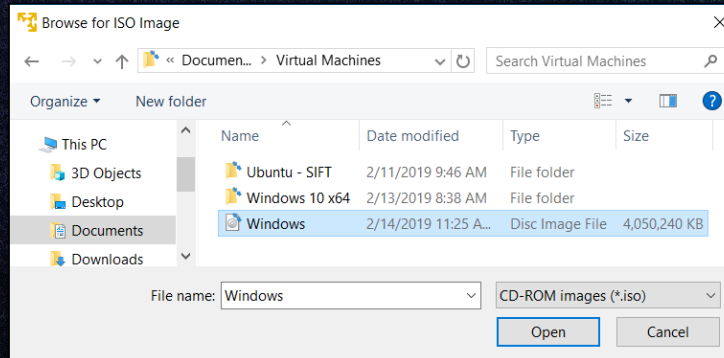
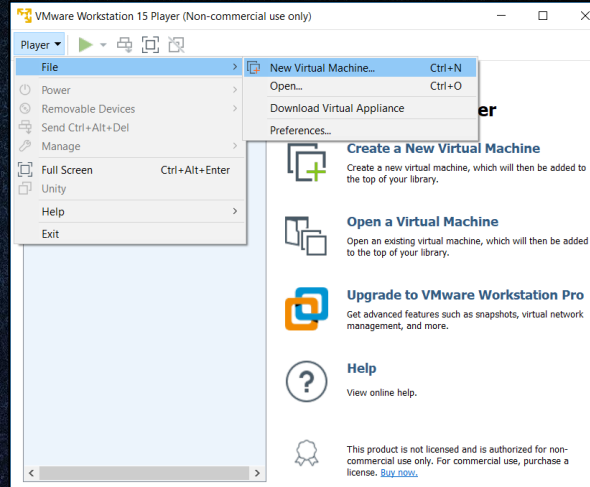
Name ↑↓	Product category ↑↓	Operating System ↑↓	System type ↑↓	Language
Windows 10 Assessment and Deployment Kit	Operating System	Windows	64 bit	English
Windows 10 Assessment and Deployment Kit, version 1903	Operating System	Windows	64 bit	English
Windows 10 Education N, Version 1809 (Updated Sept 2018)	Operating System	Windows	64 bit	English
Windows 10 Education, Version 1809 (Updated Sept 2018)	Operating System	Windows	64 bit	English

Windows ISO Download

7CNRC-8C867-WDKYQ-YWRCQ-DV64M



Windows VM Installation



Windows VM Installation Settings

New Virtual Machine Wizard

Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:

Location:

New Virtual Machine Wizard

Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB):

Recommended size for Windows 10 x64: 60 GB

☒ Store virtual disk as a single file
☐ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Windows VM Installation

New Virtual Machine Wizard

Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:

Location:

New Virtual Machine Wizard

Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

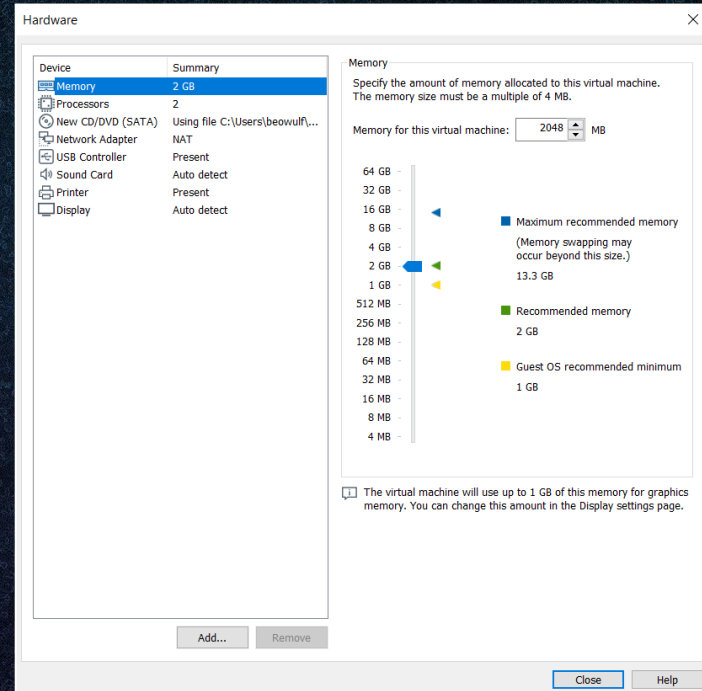
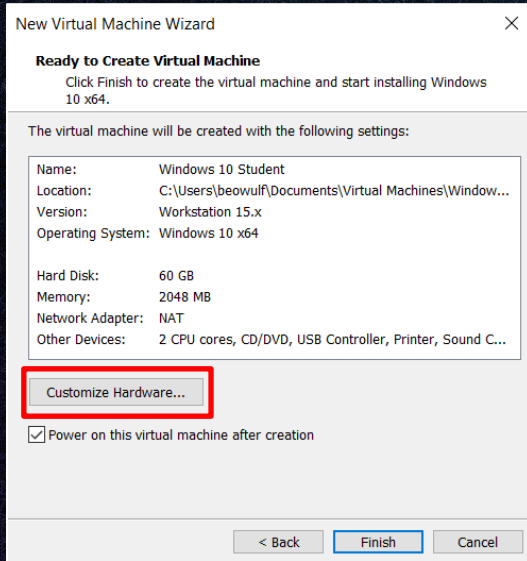
Maximum disk size (GB):

Recommended size for Windows 10 x64: 60 GB

☒ Store virtual disk as a single file
☐ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

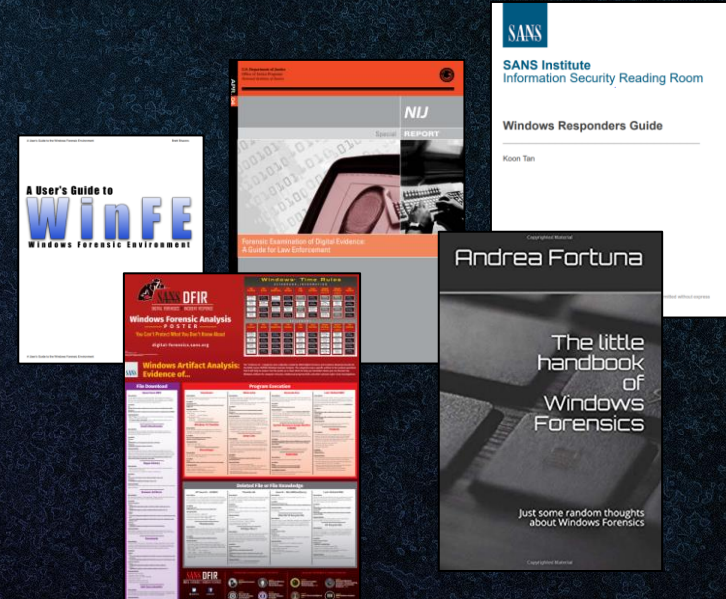
Windows VM Installation



Forensic Investigation Best Practices

Forensics Analysis Best Practices

- There are numerous sources for forensics best practices from security experts in numerous fields
- Many sources are compiled with security testing in mind:
 - ✓ SANS DFIR
 - ✓ SANS Reading Room
 - ✓ Windows Forensics Best Practices
 - ✓ Forensics Legal Considerations



Incident Response Activities

- We can classify forensic and response activities into the following steps:
 - ✓ Conduct Initial Response
 - ✓ Evidence Gathering
 - ✓ Protect Volatile Information
 - ✓ Create a Forensics Response Toolkit
 - ✓ Gather Physical & Digital Evidence
 - ✓ Script Data Collection
 - ✓ Identify Footprints
- Organizations should consider the following activities prior to responding to a forensic investigation
 - ✓ Response Policy
 - ✓ Subject Matter Expertise
 - ✓ Personnel Training
 - ✓ Forensic Testing Environment
 - ✓ Organizational Exercises

Conduct Initial Response

- Forensics investigations are generally conducted when one or more incidents occur:
 - ✓ Security Breach
 - ✓ Data Exfiltration
 - ✓ Successful Social Engineering
- Several questions need to be asked during this process:
 - ✓ Who found the incident?
 - ✓ How was the incident discovered?
 - ✓ When did the incident occur?
 - ✓ What was the level of damage?
 - ✓ Where was the attack initiated?
 - ✓ What techniques were being used to compromise the system?
- Before any technical solutions are applied the scope of the investigation must be determined

Evidence Gathering

- When collecting evidence, investigators should conduct as few activities on the system as possible and maintain detailed evidence documentation to include all steps conducted
- Incident response and forensic collection policies should address chain of custody
- During the initial evidence gathering process we should not:
 - ✓ Overwrite original media
 - ✓ Kill any processes
 - ✓ Manipulate timestamps
 - ✓ Utilize untrusted collection or analysis tools
 - ✓ Perform any system modifications including:
 - Reboot
 - Patching
 - Updating
 - Reconfiguring

Protect Volatile Information

- Recall in an earlier discussion we spoke of the order of volatility (OOV) of a system
- With a Windows forensic analysis, OOV also applies and includes:
 - ✓ CPU Registers & Cache
 - ✓ RAM Contents
 - ✓ Network Connections
 - ✓ Running Processes
 - ✓ Hard Drive File System
 - ✓ Removable and Backup Media

Critical Volatile Information

- The most critical information contained in volatile memory includes:
 - ✓ System Timestamps
 - ✓ Running and Active Processes
 - ✓ Network Connections
 - ✓ Port Status
 - Open
 - Listening
 - Connected
 - Time Wait
 - ✓ Current logon users

Create a Forensics Response Toolkit

- There are numerous tools available for forensic investigations and it is critical to vet all tools prior to deploying them in a live environment
- Forensic analysis teams should consolidate tools into a single repository and ensure all software dependences are accounted for
 - ✓ Live distribution – DVD, External Media
 - ✓ Github – Online repository
- To ensure corrupting artifacts are not introduced to the target system process detection tools (i.e. Process Monitor) can be utilized to ensure system modification does not occur

Windows-Based Response Toolkit Tools

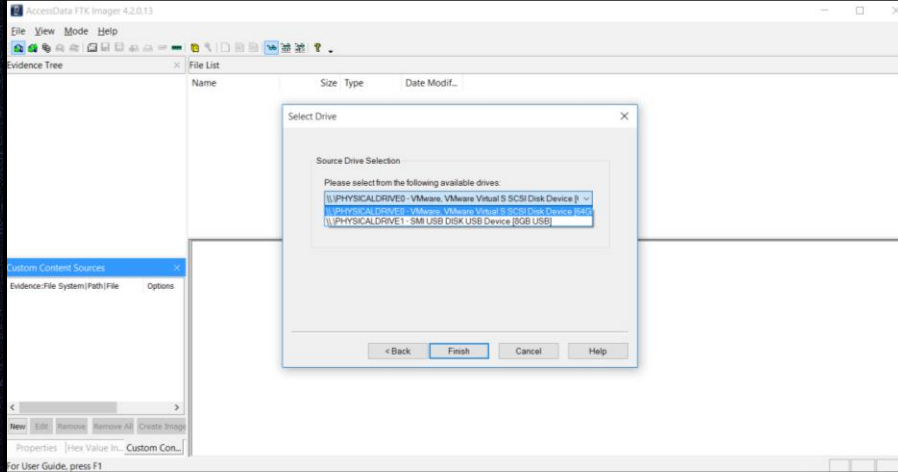
Tools	Description	Where to get
cmd.exe	Command prompt.	From a trusted system
ipconfig	A system tool that enumerates IP address of the system.	From a trusted system
netstat	A system tool that enumerates listening ports and network connections.	From a trusted system
nbstat	A system tool that displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache.	From a trusted system
date	A system tool that enumerates the system date.	From a trusted system
time	A system tool that enumerates the system time.	From a trusted system
env	A utility that enumerates system variables.	http://unxutils.sourceforge.net/
psuptime	A utility that tells you how long a Win NT/2K system has been up.	http://www.sysinternals.com/ntw2k/freeware/psuptime.shtml
net	A system tool that enumerates NetBIOS connections, user accounts, share folders, start services etc.	From a trusted system
psloggedon	A utility that shows all users connected locally and remotely.	http://www.sysinternals.com/ntw2k/freeware/psloggedon.shtml
pulist	A command-line tool that displays active processes running on local or remote computers. It also captures the user running the processes.	http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/pulist-o.asp
pslist	A command-line tool shows CPU-oriented information for all the processes that are currently running on the local system. The information listed for each process includes the time the process has executed, the amount of time the process has executed in kernel and user modes, and the amount of physical memory that the OS has assigned the process. Command-line switches allow you to view memory-oriented process information, thread statistics, or all three types of data.	http://www.sysinternals.com/ntw2k/freeware/pslist.shtml
listdlls	A utility that list all the DLLs that are currently loaded, including where they are loaded and their version numbers.	http://www.sysinternals.com/ntw2k/freeware/listdlls.shtml
fport	A utility that identify open ports and their associated applications.	http://www.foundstone.com/resources/intrusion_detection.htm

psservice	A utility that displays the status, configuration, and dependencies of a service, and allows you to start, stop, pause, resume and restart them.	http://www.sysinternals.com/ntw2k/freeware/psservice.shtml
psinfo	A command-line tool that gathers key information about the local or remote Windows NT/2000 system, including the type of installation, kernel build, registered organization and owner, number of processors and their type, amount of physical memory, the install date of the system, and if it's a trial version, the expiration date.	http://www.sysinternals.com/ntw2k/freeware/psinfo.shtml
arp	A system tool that maps the logical IP address to physical MAC address.	From a trusted system
hfind	A utility that find files that have hidden attribute set.	http://www.foundstone.com/resources/proddesc/forensic-toolkit.htm
streams	A utility to view NTFS file stream information.	http://www.sysinternals.com/ntw2k/source/misc.shtml
ntlast	A utility that monitors successful and failed login to the system.	http://www.foundstone.com/resources/proddesc/ntlast.htm
reg	A command-line registry manipulation. Allow you to query the registry entries.	From trusted NT Resource Kit
auditpol	A command-line tool that determines the audit policy on a system.	From trusted NT Resource Kit
regdmp	A command-line tool that dumps the registry as a text file.	From trusted NT Resource Kit
md5sum	A utility that generated a hash value of a file.	http://unxutils.sourceforge.net/
netcat (nc)	A utility that reads and writes data across network connections. Netcat is an equivalent version of netcat but create an encrypted channel of communication.	http://www.atstake.com/research/tools/network_utilities/
cat	A utility that is the equivalent of cat in the Unix world.	http://unxutils.sourceforge.net/
find	A utility that is the equivalent of find in the Unix world.	http://unxutils.sourceforge.net/
grep	A utility that is the equivalent of grep in the Unix world.	http://unxutils.sourceforge.net/
filemon	A utility that monitors and displays file system activity on a system in real-time. It allows one to explore the way Windows works, seeing how applications use the files and DLLs.	http://www.sysinternals.com/ntw2k/source/filemon.shtml
clip	A utility that put the Windows clipboard text to stdout.	http://unxutils.sourceforge.net/
tcpdump windump	A tool for network sniffer/analyzer. Windump is the Windows platform for tcpdump.	http://www.tcpdump.org/ http://windump.polito.it/

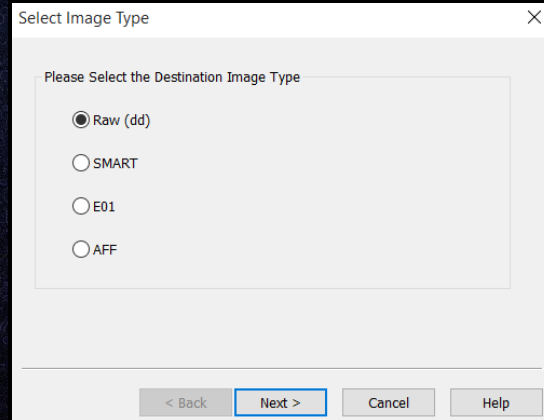
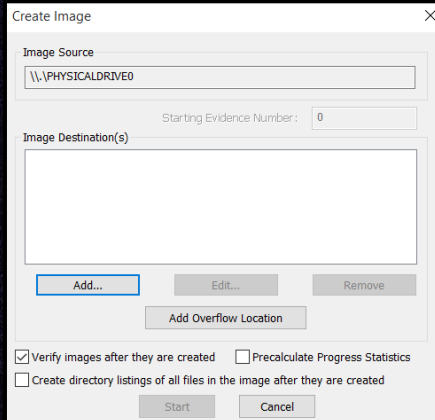
Gather Evidence

- **Evidence Gathering Steps**
 - ✓ **On External Collection System**
 - **Collect System Image**
 - **Hash Image**
 - ✓ **On Target System**
 - **Open a Trusted Command Shell**
 - **Prepare the Collection System**
 - **Collect Volatile Evidence**
 - **Collect Pertinent Logs**
 - **Perform additional network surveillance**

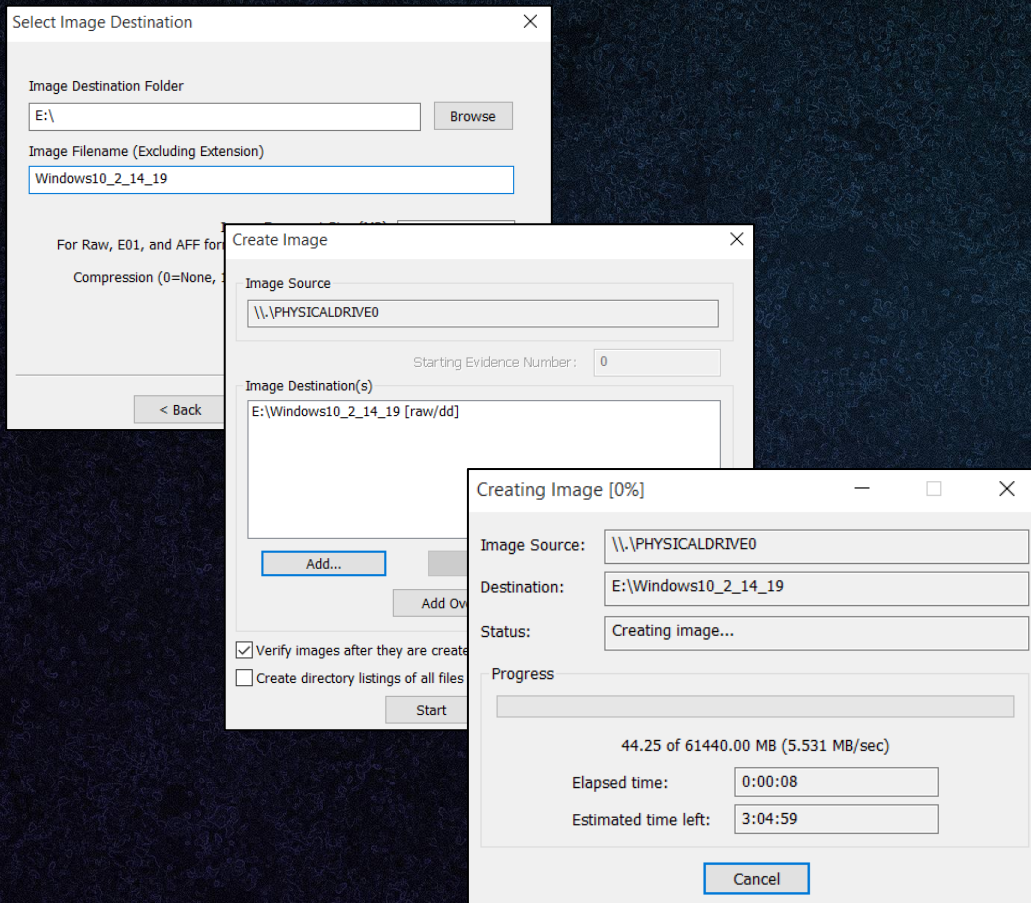
Collect System Image – Removable Media



- Select drive for collection
- Select image format



Collect System Image



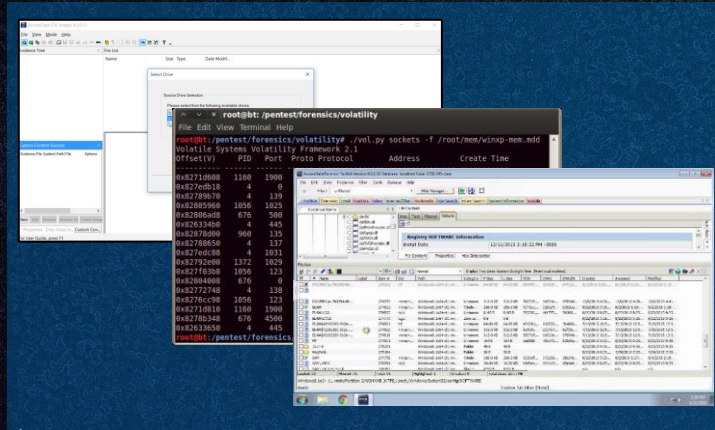
- Specify investigation specific information

Windows-Specific Volatile Artifacts

- Volatile evidence includes:
 - ✓ System Information
 - ✓ Running Processes
 - ✓ Open Sockets
 - ✓ Network Connections
 - ✓ Network Shares
 - ✓ Network Users
- On Windows systems, a batch file or Powershell script can be executed with the results stored on removable media
- The key is to minimize interaction with the target system

```
WindowsCommands.bat
1 date /t
2 time /t
3 ipconfig /all
4 env
5 psinfo
6 psuptime
7 psloggedon
8 ntlast -r
9 ntlast -f
10 net use
11 net session
12 net file
13 net share
14 net view
15 net user
16 net accounts
17 net localgroup
18 net start
19 nbtstat -n
20 nbtstat -c
21 nbtstat -s
22 pclip
23 pslist
24 pulist
25 psservice
26 listdlls
27 fport
28 netstat -an
29 netstat -rn
30 arp -a
31 dir /t:a /a /s /o:d c:
32 dir /t:w /a /s /o:d c:
33 dir /t:c /a /s /o:d c:
34 hfind c:
```


Collect Volatile Evidence – Removable Media



Toolkit



Target System



Analysis System

Analyze Volatile Evidence – Removable Media



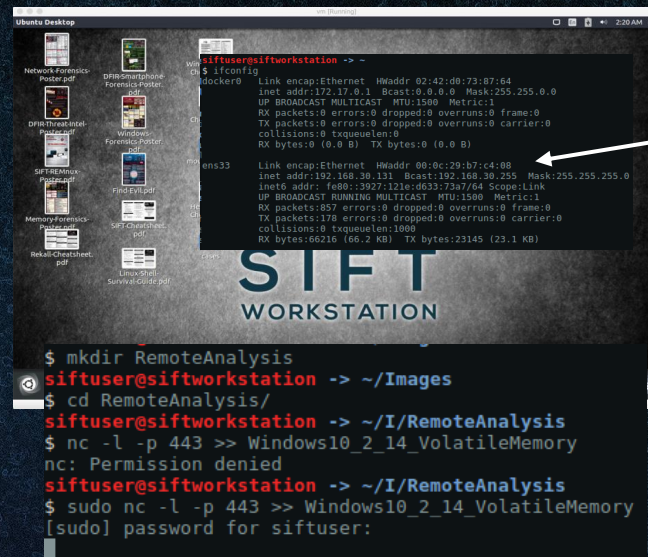
Collect Volatile Evidence – Remote Connection



```
E:\nc>..\WindowsCommands.bat | nc.exe 192.168.30.131 443
```



Target System



IP Address

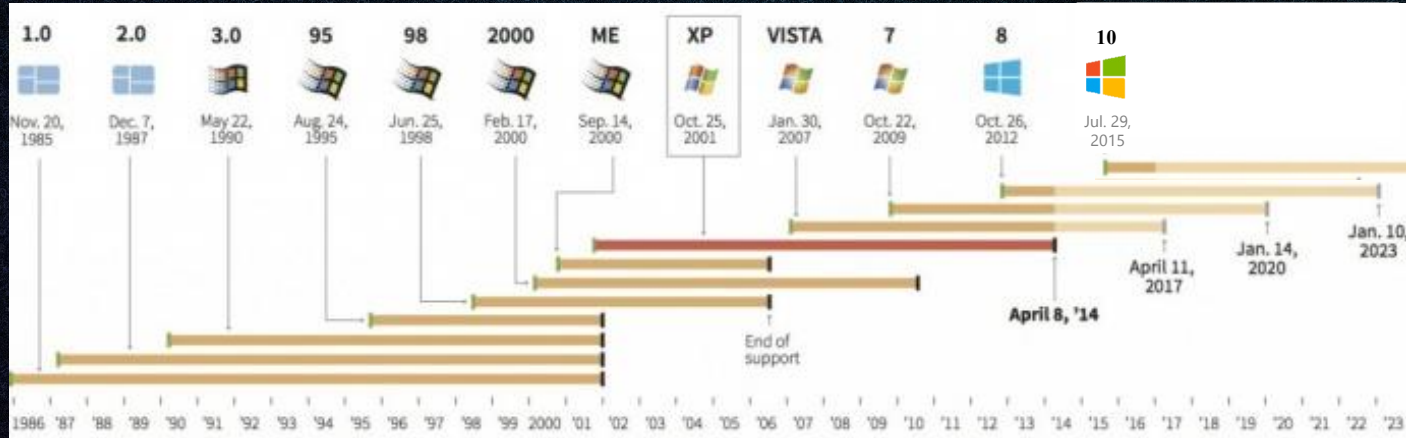
Requires Elevated Privileges



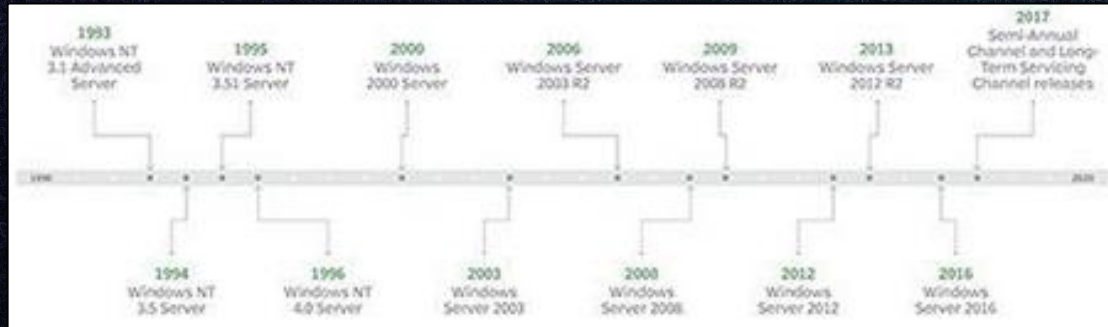
Analysis System

Introduction to the Windows Operating System

Windows Operating System Version Timeline



Desktop / Laptop



Server

Windows Operating System Versions

- It is not unusual to see Windows versions as early as:
 - Windows NT 4.0
 - Windows 95/98
 - Windows XP
 - Windows Server 2003
- Organizations maintain copies of both physical and virtualized Windows systems for numerous reasons:
 - Cost
 - Labor
 - Backwards Capability
 - Applications No Longer in Development
- Forensic analysts should train on older interacting with all versions of Windows

Windows Operating System Modes

- **Windows is separated into two modes:**
 - ✓ **User Mode**
 - User mode does not directly access underlying hardware or reference memory addresses
 - Access to hardware or memory requires Application Programming Interfaces (API)
 - User mode crashes are recoverable
 - ✓ **Kernel Mode**
 - Kernel mode has unrestricted access to the underlying hardware and can directly reference memory addresses
 - Reserved for trusted functions in the operating system
 - Kernel mode crashes are generally unrecoverable
- **The CPU is configured to separate of user and kernel mode operation to prevent access to running processes**

Windows OS Digital Artifacts

- Up to this point in the course the focus has been on the underlying file systems of the Windows OS
 - ✓ FATX
 - ✓ NTFS
- If we now consider the Windows OS, the file system will be augmented with additional artifacts:
 - ✓ Windows Registry
 - Shell Bags
 - ✓ Event Logs
 - ✓ Recycle Bin
 - ✓ Prefetch Files
 - ✓ Scheduled Tasks
 - ✓ Jump Lists
 - ✓ Application Files

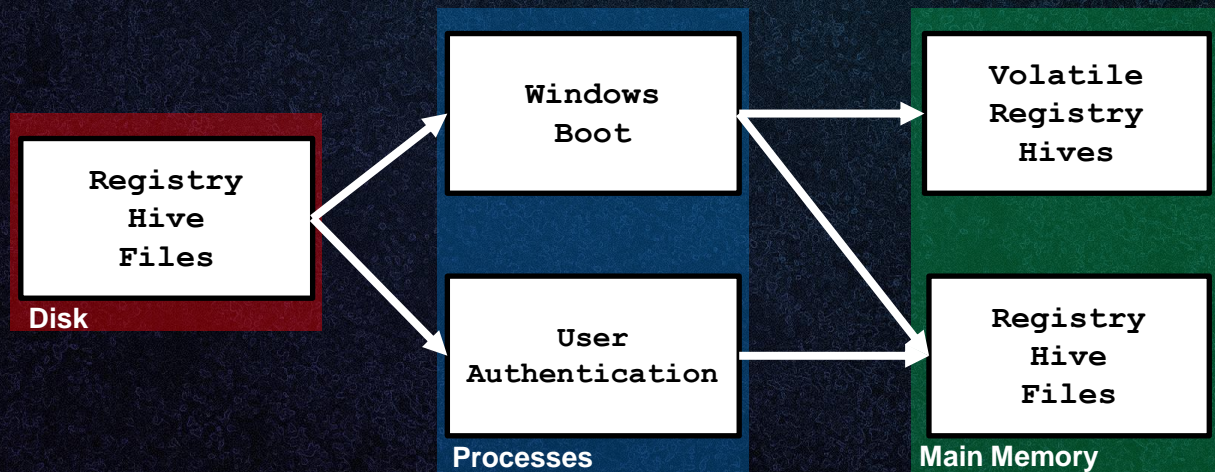
Introduction to the Windows Registry

Windows Registry Details

- The Windows registry is a “central hierarchal database used to store information that is necessary to configure the system for one or more users, applications, and hardware devices.”
- Prior to Windows 2000, initialization files were used for system configuration
 - ✓ boot.ini
 - ✓ system.ini
 - ✓ win.ini
- Since Windows 2000, a registry structure was utilized to create a more efficient interaction between kernel and user functions
- Registry entries contain two different structures:
 - Registry Key
 - Similar to a folder in that holds multiple values
 - Registry Value
 - Similar to a file that contains specific values

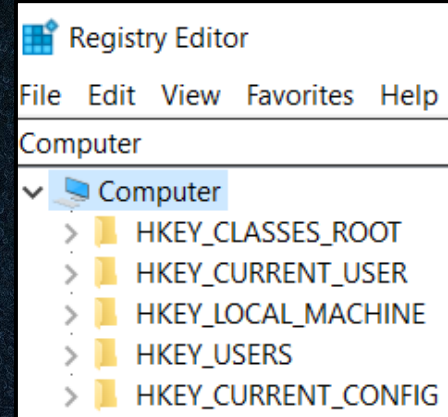
Windows Registry Operation

- A comprehensive copy of the registry can only be found in main memory since it requires both the registry entries along with active processes that create it
- From a forensics standpoint, this is significant because gathering a complete registry requires live memory capture



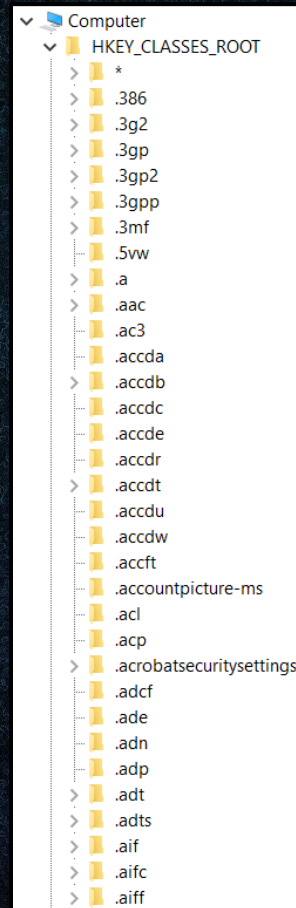
Windows Registry Hives

- The Windows registry contains hierarchical root keys
 - ✓ HKEY_CLASSES_ROOT (HKCR)
 - All information relating to file name extensions and Object Linking and Embedding (OLE)
 - ✓ HKEY_CURRENT_USER (HKCU)
 - Contains settings for the currently logged on user
 - ✓ HKEY_LOCAL_MACHINE (HKLM)
 - Contains information about hardware and software on the system
 - ✓ HKEY_USERS (HKU)
 - Contains information of different user settings and consolidated from HKCU
 - ✓ HKEY_CURRENT_CONFIG (HKCC)
 - Contains information about current hardware configurations
 - Usually empty until loaded during the boot process and loads hardware profiles into HKLM sub keys

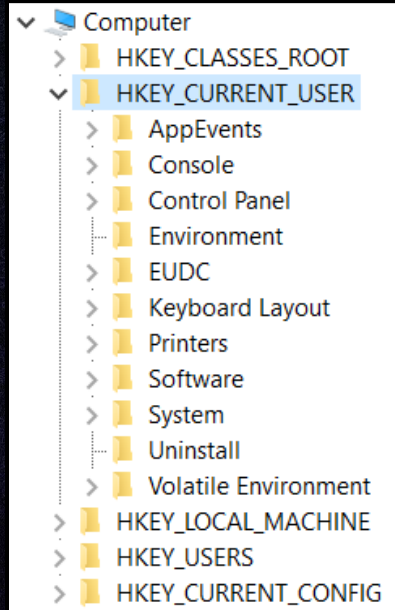


HKEY_CLASSES_ROOT

- Most of the Windows Registry is composed of HKCR entries
- HKCR contains extension associations and describes how files operate with applications and is composed of two hives:
 - HKLM\SOFTWARE\Classes - Machine-based defaults
 - HKCU\Software\Classes - User-based
- The HKCR hive contains data relative to:
 - User Settings
 - File Associations
 - Component Object Model (COM) Objects (i.e. IPC)
 - Programmatic Identifiers (ProgID)
 - Example: HKCR\avi\OpenWithProgIds
 - Class ID (CLSID)
 - Example: HKCR\CLSID
 - Interface ID (IID)
 - Example: HKCR\Interface



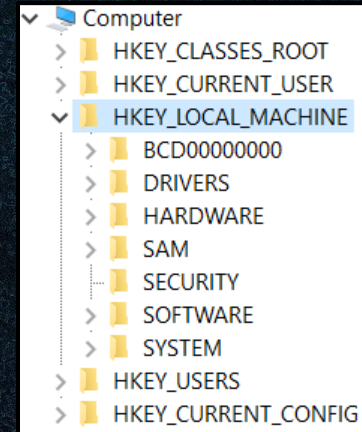
HKEY_CURRENT_USER



- HKCU changes each time a user logs into the OS
- Each user profile contains configurations for:
 - ✓ Groups
 - ✓ Network Connections
 - ✓ Desktop Settings
 - ✓ External Peripherals
- Each user HKCU data feeds into HKEY_USERS

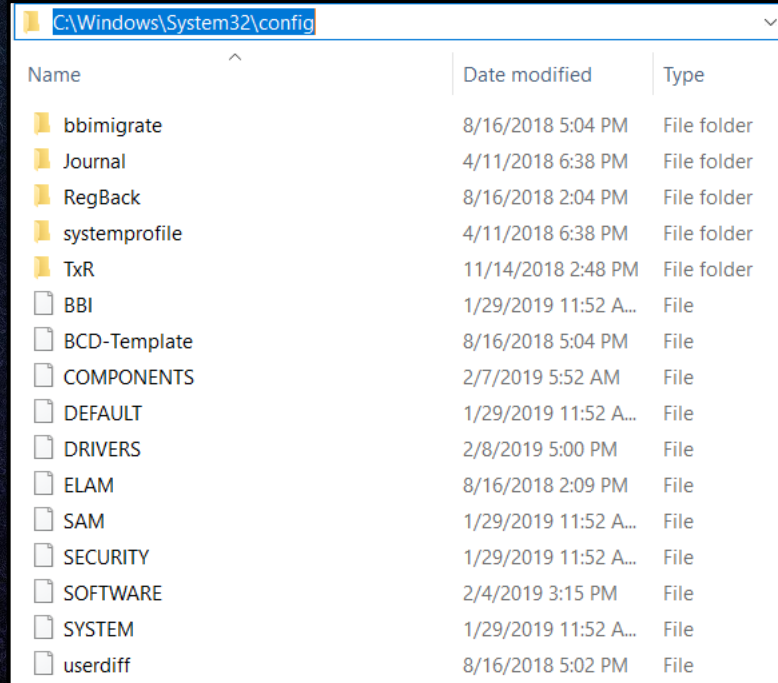
HKEY_LOCAL_MACHINE

- **HKLM contains hardware, driver, and software configuration data:**
 - ✓ **HKLM\Hardware – Visible Subkey**
 - Data relative to CPU, BIOS, and hardware devices
 - ✓ **HKLM\Software – Visible Subkey**
 - Alphabetical listing of software vendors
 - When an application starts, data is written here
 - Used to find user security identifiers (SID)
 - ✓ **HKLM\SAM – Hidden Subkey**
 - **Security Accounts Manager (SAM)** is a database of domain information including aliases, usernames, accounts, and password hashes
 - Only accessible through system account
 - PSEXec
 - ✓ **HKLM\Security – Hidden Subkey**
 - Stores current user security policy and is linked to either domain or local security database
 - Only accessible through system account
 - PSEXec



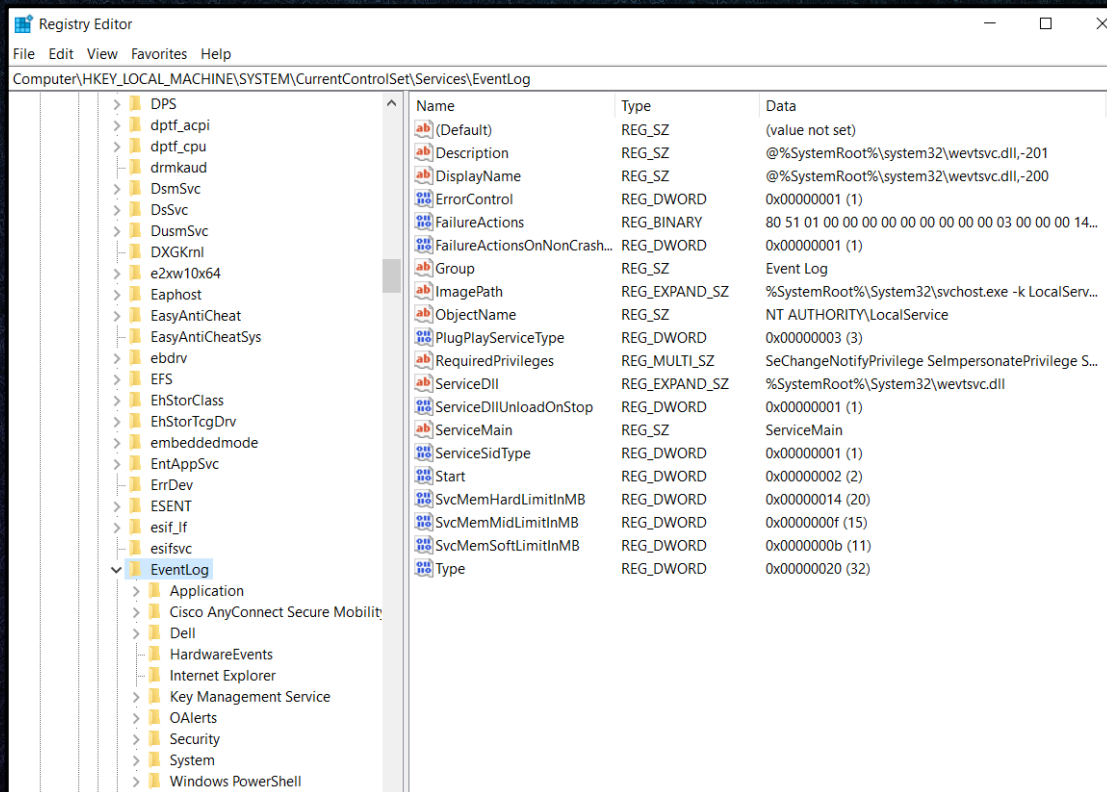
HKEY_LOCAL_MACHINE

- HKLM subkeys can be found in:
 - ✓ C:\Windows\System32\config



Name	Date modified	Type
bbimigrate	8/16/2018 5:04 PM	File folder
Journal	4/11/2018 6:38 PM	File folder
RegBack	8/16/2018 2:04 PM	File folder
systemprofile	4/11/2018 6:38 PM	File folder
TxR	11/14/2018 2:48 PM	File folder
BBI	1/29/2019 11:52 A...	File
BCD-Template	8/16/2018 5:04 PM	File
COMPONENTS	2/7/2019 5:52 AM	File
DEFAULT	1/29/2019 11:52 A...	File
DRIVERS	2/8/2019 5:00 PM	File
ELAM	8/16/2018 2:09 PM	File
SAM	1/29/2019 11:52 A...	File
SECURITY	1/29/2019 11:52 A...	File
SOFTWARE	2/4/2019 3:15 PM	File
SYSTEM	1/29/2019 11:52 A...	File
userdiff	8/16/2018 5:02 PM	File

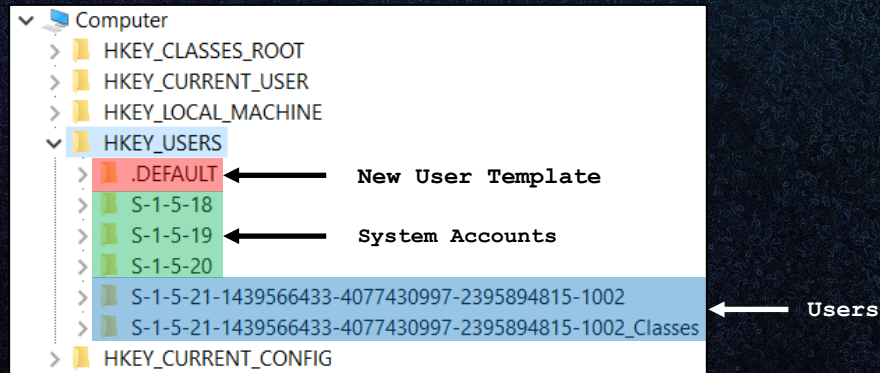
HKEY_LOCAL_MACHINE – Event Logs



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog

HKEY_USERS

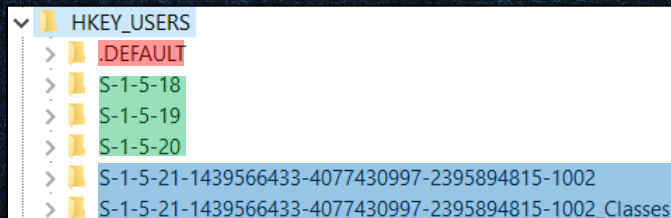
- HKEY_USERS registry hive tracks users with a security ID (SID)
- Keys and values under each SID specifies settings such as:
 - ✓ Environment Variables
 - ✓ Mapped Drives
 - ✓ Desktop Configuration
- During user login, settings are loaded into main memory
- Additional registry keys in HKLM help identify SIDs:
 - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList



HKEY_USERS SID

- The Windows Command Line Utility (WMIC) can be used to identify system and user accounts:

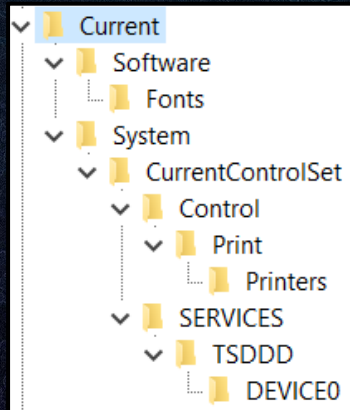
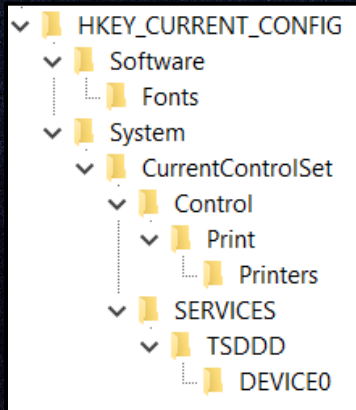
```
C:\>wmic sysaccount get sid, name
Name                               SID
Everyone                           S-1-1-0
LOCAL                              S-1-2-0
CREATOR OWNER                       S-1-3-0
CREATOR GROUP                      S-1-3-1
CREATOR OWNER SERVER                S-1-3-2
CREATOR GROUP SERVER                S-1-3-3
OWNER RIGHTS                        S-1-3-4
DIALUP                             S-1-5-1
NETWORK                             S-1-5-2
BATCH                               S-1-5-3
INTERACTIVE                         S-1-5-4
SERVICE                           S-1-5-6
ANONYMOUS LOGON                     S-1-5-7
PROXY                               S-1-5-8
SYSTEM                             S-1-5-18
ENTERPRISE DOMAIN CONTROLLERS       S-1-5-9
SELF                                S-1-5-10
Authenticated Users                  S-1-5-11
RESTRICTED                           S-1-5-12
TERMINAL SERVER USER                S-1-5-13
REMOTE INTERACTIVE LOGON             S-1-5-14
IUSR                                 S-1-5-17
LOCAL SERVICE                       S-1-5-19
NETWORK SERVICE                     S-1-5-20
BUILTIN                              S-1-5-32
```



```
C:\>wmic useraccount get sid, name
Name                               SID
Administrator                      S-1-5-21-1439566433-4077430997-2395894815-500
beowulf                             S-1-5-21-1439566433-4077430997-2395894815-1002
DefaultAccount                      S-1-5-21-1439566433-4077430997-2395894815-503
Guest                               S-1-5-21-1439566433-4077430997-2395894815-501
WDAGUtilityAccount                  S-1-5-21-1439566433-4077430997-2395894815-504
```

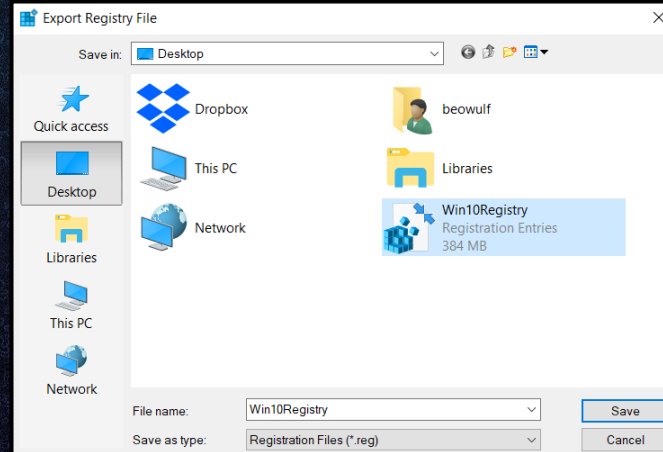
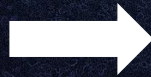
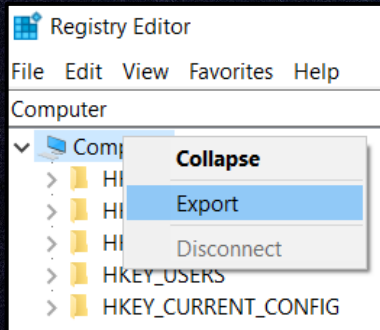

HKEY_CURRENT_CONFIG

- Unlike the other hives, HKCC does not contain native keys and values
- HKCC is an HKLM key shortcut that tracks hardware configurations
 - HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current
- Changes to either HKCC or the HKLM hardware hive changes the other



Exporting Windows Registry

- Windows registry collection can be of specific registry hives or the entire database
- There are numerous collection methods
 - ✓ Direct Registry Export
 - ✓ Live Registry Image
 - ✓ Dead Registry Image



Collect Registry Hives

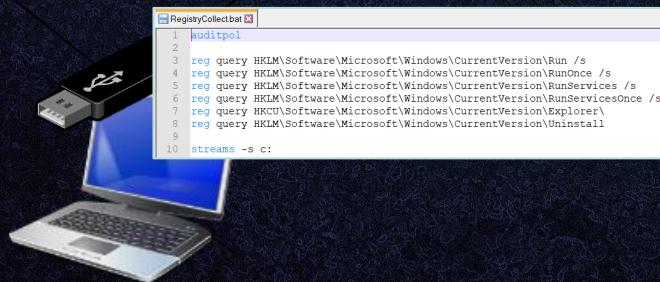


```
E:\nc>..\RegistryCollect.bat | nc.exe 192.168.30.131 443
```



```
siftuser@siftworkstation -> ~/I/RemoteAnalysis  
$ sudo nc -l -p 443 >> Windows10_2_14_Registry  
[sudo] password for siftuser:
```

Requires Elevated Privileges



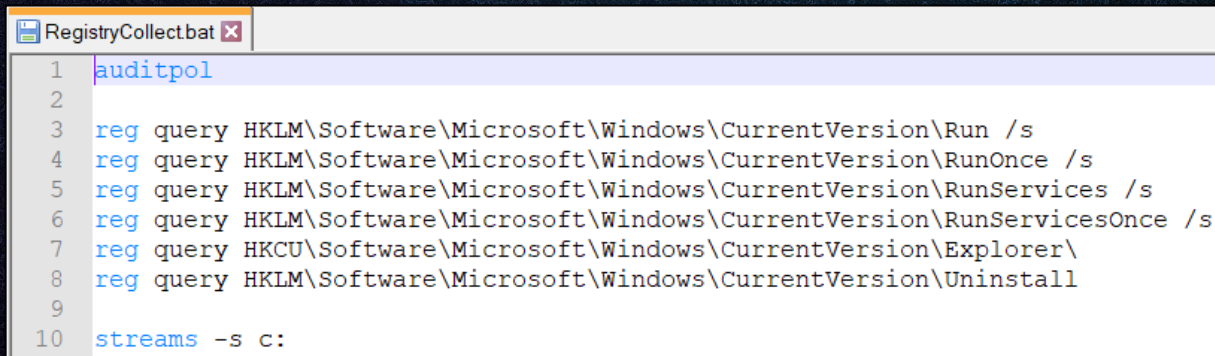
Target System



Analysis System

Windows Registry Query List

- The registry query strings can be configured to query each hive or specific keys and values
- A tailored list should be developed based on the specifics of each test event



```
1 auditpol
2
3 reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run /s
4 reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce /s
5 reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices /s
6 reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce /s
7 reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\
8 reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall
9
10 streams -s c:
```


Windows Registry Shellbags

- Inside of the registry there are keys that configure the folder dimensions such as size, view, icon, and position
- From a forensic standpoint these values are incredibly valuable since these values provide persistent information on when folders and applications were used and allows tracking of previously mounted volumes, deleted files, and user actions
- Shellbag registry key:
 - ✓ `HEKY_USERS\{USERID}\Local Settings\Software\Microsoft\Windows\Shell`

Windows Registry Analysis Tools

➤ There are a number of helpful Windows Registry collection and analysis tools including:

✓ FTK Registry Viewer

- Demo and commercial registry viewer from AccessData

✓ RegRipper

- Perl-based Windows Registry data extraction tool

✓ BulkExtractor

- High speed disk scanner that analyzes disk images, files, or directories without the need of file system

Computer Forensics Tool Catalog

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Home Tool Search Forensic Tool Taxonomy Vendors Contacts

Home > Tool Search

Search for forensic tools by functionality

☐ find all Windows Registry Analysis tools ☐ refine by search parameters

Forensic Tool Functionalities

- Case Review
- Cloud Services
- Data Analytics
- Database Forensics
- Deleted File Recovery
- Disk Cataloging
- Disk Imaging
- Drone Forensics
- Email Parsing
- File Carving

Forensic Functionality: Windows Registry Analysis

Technical Parameters:

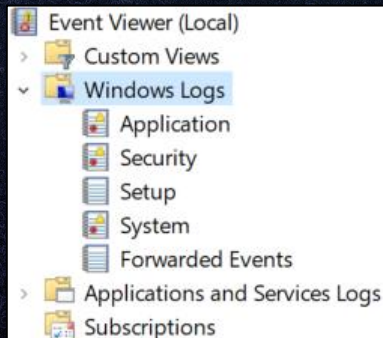
Tool host OS / runtime environment:	Input data type(s):	Automated hive extraction and parsing:	Registry rebuilding:	Deleted key recovery:
any Windows Mac Linux	any raw (dd) EnCase Evidence File Format Version 2 (.ex01) Expert Witness (.e01)	any active Registry active file system Windows restore points	any supports Registry rebuilding Registry rebuilding unsupported	any supports deleted key recovery deleted key recovery unsupported

Search

Additional Windows Artifacts

Windows Artifacts – Event Logs

- Windows event logs track changes for numerous applications throughout the OS including:
 - ✓ Application
 - ✓ Security
 - ✓ Setup
 - ✓ System
 - ✓ Forwarded Events
- All details relative to how event logs are managed are handled in the Windows registry
- Windows log event IDs are used to classify different log levels



Artifacts – Recycle Bin

➤ The collection of artifacts from the recycle bin depend on which version of Windows is being analyzed

✓ **Recycle Bin Path**

- Windows 95, 98, and ME – C:\RECYCLED
- Windows NT, 2000, XP – C:\RECYCLER
- Windows Vista, 7, 8, 10 – C:\\$Recycle.Bin

✓ **Metadata File Contents**

- Windows 95, 98, ME – C:\RECYCLED\INFO2
- Windows NT, 2000, XP – C:\RECYCLER\SID*\INFO2
- Windows Vista, 7, 8, 10 – C:\\$Recycle.Bin\SID*\\$lxx

○ **Deleted File Contents**

- Windows Vista, 7, 8, 10 – C:\\$Recycle.Bin\SID*\\$Rxx

```
C:\>dir /a
Volume in drive C is OS
Volume Serial Number is DC17-F6A1

Directory of C:\

08/16/2018  01:09 PM  <DIR>          $Recycle.Bin
```


Recycle Bin Artifact Recovery

➤ Metadata File Contents

- ✓ Windows Vista, 7, 8, 10 – C:\\$Recycle.Bin\SID*\\$Ixx

➤ Deleted File Contents

- ✓ Windows Vista, 7, 8, 10 – C:\\$Recycle.Bin\SID*\\$Rxx

```
C:\$Recycle.Bin>dir /a
Volume in drive C is OS
Volume Serial Number is DC17-F6A1
```

Directory of C:\\$Recycle.Bin

```
08/16/2018  01:09 PM    <DIR>        .
08/16/2018  01:09 PM    <DIR>        ..
08/16/2018  01:09 PM    <DIR>        S-1-5-18
08/15/2018  01:01 PM    <DIR>        S-1-5-21-1439566433-4077430997-2395894815-1000
08/15/2018  11:15 AM    <DIR>        S-1-5-21-1439566433-4077430997-2395894815-1001
02/11/2019  08:28 PM    <DIR>        S-1-5-21-1439566433-4077430997-2395894815-1002
06/06/2018  02:26 AM    <DIR>        S-1-5-21-1439566433-4077430997-2395894815-500
               0 File(s)                0 bytes
               7 Dir(s)  35,597,361,152 bytes free
```

← Current User

← Admin

Recycle Bin User Ownership

➤ Identification of user account and associated security identifier

```
C:\$Recycle.Bin>wmic useraccount get name,sid
Name                SID
Administrator       S-1-5-21-1439566433-4077430997-2395894815-500
beowulf              S-1-5-21-1439566433-4077430997-2395894815-1002
DefaultAccount       S-1-5-21-1439566433-4077430997-2395894815-503
Guest                S-1-5-21-1439566433-4077430997-2395894815-501
WDAGUtilityAccount   S-1-5-21-1439566433-4077430997-2395894815-504
```

➤ Demonstration of user account access

```
C:\$Recycle.Bin>cd S-1-5-21-1439566433-4077430997-2395894815-500
Access is denied.
```

```
C:\$Recycle.Bin>cd S-1-5-21-1439566433-4077430997-2395894815-501
The system cannot find the path specified.
```

```
C:\$Recycle.Bin>cd S-1-5-21-1439566433-4077430997-2395894815-503
The system cannot find the path specified.
```

```
C:\$Recycle.Bin>cd S-1-5-21-1439566433-4077430997-2395894815-504
The system cannot find the path specified.
```

```
C:\$Recycle.Bin>cd S-1-5-21-1439566433-4077430997-2395894815-1002
```

```
C:\$Recycle.Bin\S-1-5-21-1439566433-4077430997-2395894815-1002>
```


Recycle Bin Artifact Recovery

- \$I represents metadata for the deleted file
- \$R represents the actual data of the deleted file

```
C:\$Recycle.Bin\S-1-5-21-1439566433-4077430997-2395894815-1002>dir /a
Volume in drive C is OS
Volume Serial Number is DC17-F6A1

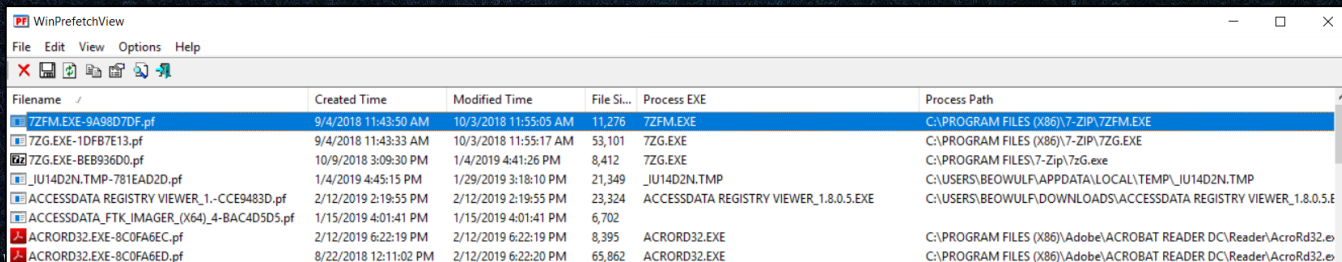
Directory of C:\$Recycle.Bin\S-1-5-21-1439566433-4077430997-2395894815-1002

02/11/2019  11:12 PM    <DIR>          .
02/11/2019  11:12 PM    <DIR>          ..
02/11/2019  11:12 PM                172 $IHZ8LX4.pdf ← Metadata
02/11/2019  11:12 PM                136 $IPVEPT9.pdf ← Metadata
02/11/2019  12:24 PM           3,780,362 $RHZ8LX4.pdf ← File Data
02/11/2019  12:25 PM           717,356 $RPVEPT9.pdf ← File Data
08/15/2018  11:17 AM                129 desktop.ini
               5 File(s)          4,498,155 bytes
               2 Dir(s)  35,580,882,944 bytes free
```

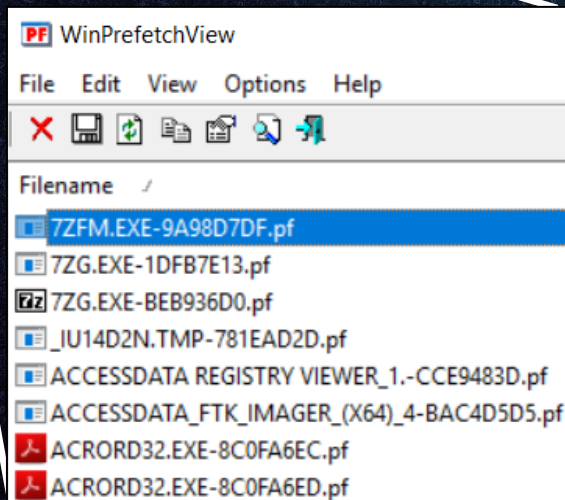

Artifacts – Prefetch Files

- Prefetch is a term used for caching of important files and libraries
- There are two types of prefetch within Windows:
 - ✓ **Boot Prefetch**
 - All versions of Windows
 - ✓ **Application Prefetch**
 - Windows XP, Vista, 7, 8, 10
 - Turned off by default on Windows Server versions
- Prefetch files can aid in identifying:
 - ✓ When users ran programs
 - ✓ When programs and files were deleted
 - ✓ Identification of malware infection
 - ✓ Building timeline analyses
 - ✓ File download times
 - ✓ Develop methods for root cause analysis

Prefetch Artifacts



Filename	Created Time	Modified Time	File Size	Process EXE	Process Path
7ZFM.EXE-9A98D7DF.pf	9/4/2018 11:43:50 AM	10/3/2018 11:55:05 AM	11,276	7ZFM.EXE	C:\PROGRAM FILES (X86)\7-ZIP\7ZFM.EXE
7ZG.EXE-1DFB7E13.pf	9/4/2018 11:43:33 AM	10/3/2018 11:55:17 AM	53,101	7ZG.EXE	C:\PROGRAM FILES (X86)\7-ZIP\7ZG.EXE
7ZG.EXE-BEB936D0.pf	10/9/2018 3:09:30 PM	1/4/2019 4:41:26 PM	8,412	7ZG.EXE	C:\PROGRAM FILES\7-Zip\7zG.exe
_IU14D2N.TMP-781EAD2D.pf	1/4/2019 4:45:15 PM	1/29/2019 3:18:10 PM	21,349	_IU14D2N.TMP	C:\USERS\BEOWULF\APPDATA\LOCAL\TEMP\IU14D2N.TMP
ACCESSDATA REGISTRY VIEWER_1.-CCE9483D.pf	2/12/2019 2:19:55 PM	2/12/2019 2:19:55 PM	23,324	ACCESSDATA REGISTRY VIEWER_1.8.0.5.EXE	C:\USERS\BEOWULF\DOWNLOADS\ACCESSDATA REGISTRY VIEWER_1.8.0.5.E
ACCESSDATA_FTK_IMAGER_(X64)_4-BAC4D5D5.pf	1/15/2019 4:01:41 PM	1/15/2019 4:01:41 PM	6,702		
ACRORD32.EXE-8C0FA6EC.pf	2/12/2019 6:22:19 PM	2/12/2019 6:22:19 PM	8,395	ACRORD32.EXE	C:\PROGRAM FILES (X86)\Adobe\ACROBAT READER DC\Reader\AcroRd32.e
ACRORD32.EXE-8C0FA6ED.pf	8/22/2018 12:11:02 PM	2/12/2019 6:22:20 PM	65,862	ACRORD32.EXE	C:\PROGRAM FILES (X86)\Adobe\ACROBAT READER DC\Reader\AcroRd32.e



Filename
7ZFM.EXE-9A98D7DF.pf
7ZG.EXE-1DFB7E13.pf
7ZG.EXE-BEB936D0.pf
_IU14D2N.TMP-781EAD2D.pf
ACCESSDATA REGISTRY VIEWER_1.-CCE9483D.pf
ACCESSDATA_FTK_IMAGER_(X64)_4-BAC4D5D5.pf
ACRORD32.EXE-8C0FA6EC.pf
ACRORD32.EXE-8C0FA6ED.pf

Application

Hash

.pf

Path

References

➤ Windows Forensics Analysis Toolkit, Carvey, 2014

➤ Windows Registry Forensics, Carvey, 2009

➤ Windows Forensics Best Practices

- ✓ http://www.campus64.com/digital_learning/data/windows_forensics/users-guide-to-winfe1.pdf
- ✓ <https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download>
- ✓ <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>

➤ Windows Registry

- ✓ <https://www.techsupportalert.com/content/deeper-windows-registry.htm>
- ✓ <https://docs.microsoft.com/en-us/windows/desktop/sysinfo/registry-hives>
- ✓ <https://support.microsoft.com/en-us/help/256986/windows-registry-information-for-advanced-users>
- ✓ <https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493923972.pdf>
- ✓ <http://www.onlinecmag.com/registry-root-keys>
- ✓ <http://www.williballenthin.com/forensics/shellbags>

➤ Windows Operating System Modes

- ✓ <https://blog.codinghorror.com/understanding-user-and-kernel-mode>