

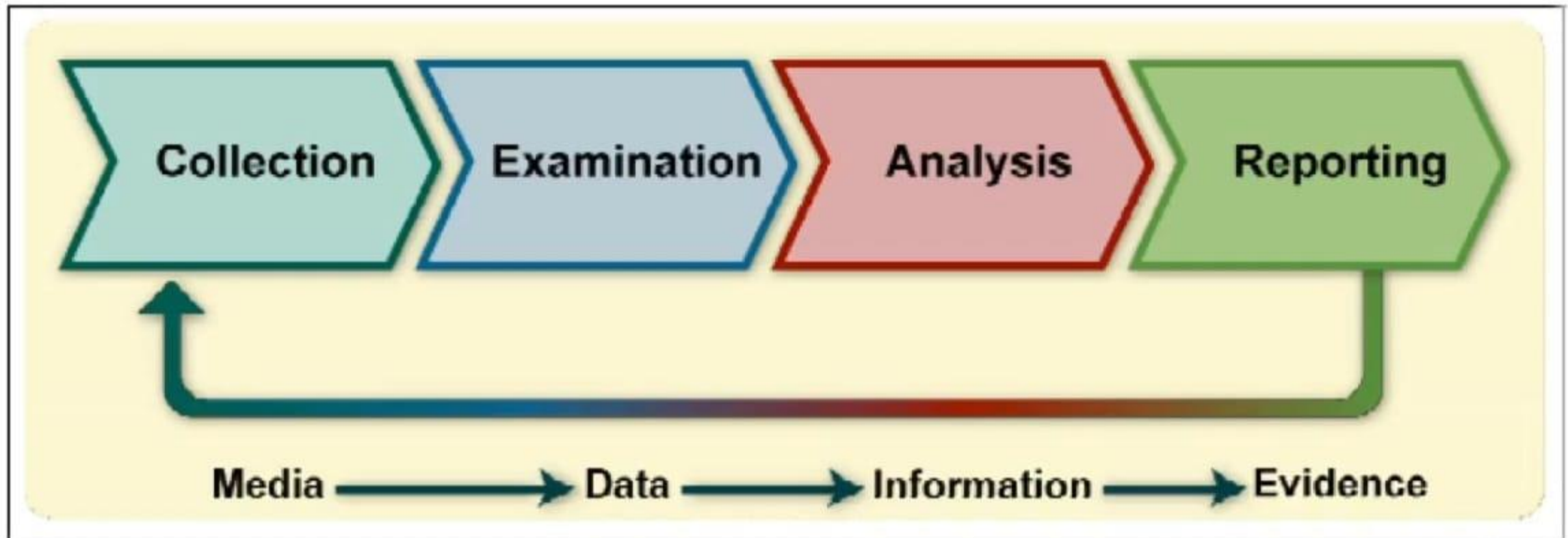
Windows Forensic

What is windows forensic

Windows Forensics, include the process of conducting or performing forensic investigations of systems which run on Windows operating systems, It includes analysis of incident response, recovery, and auditing of equipment used in executing any criminal activity.

Forensic Process

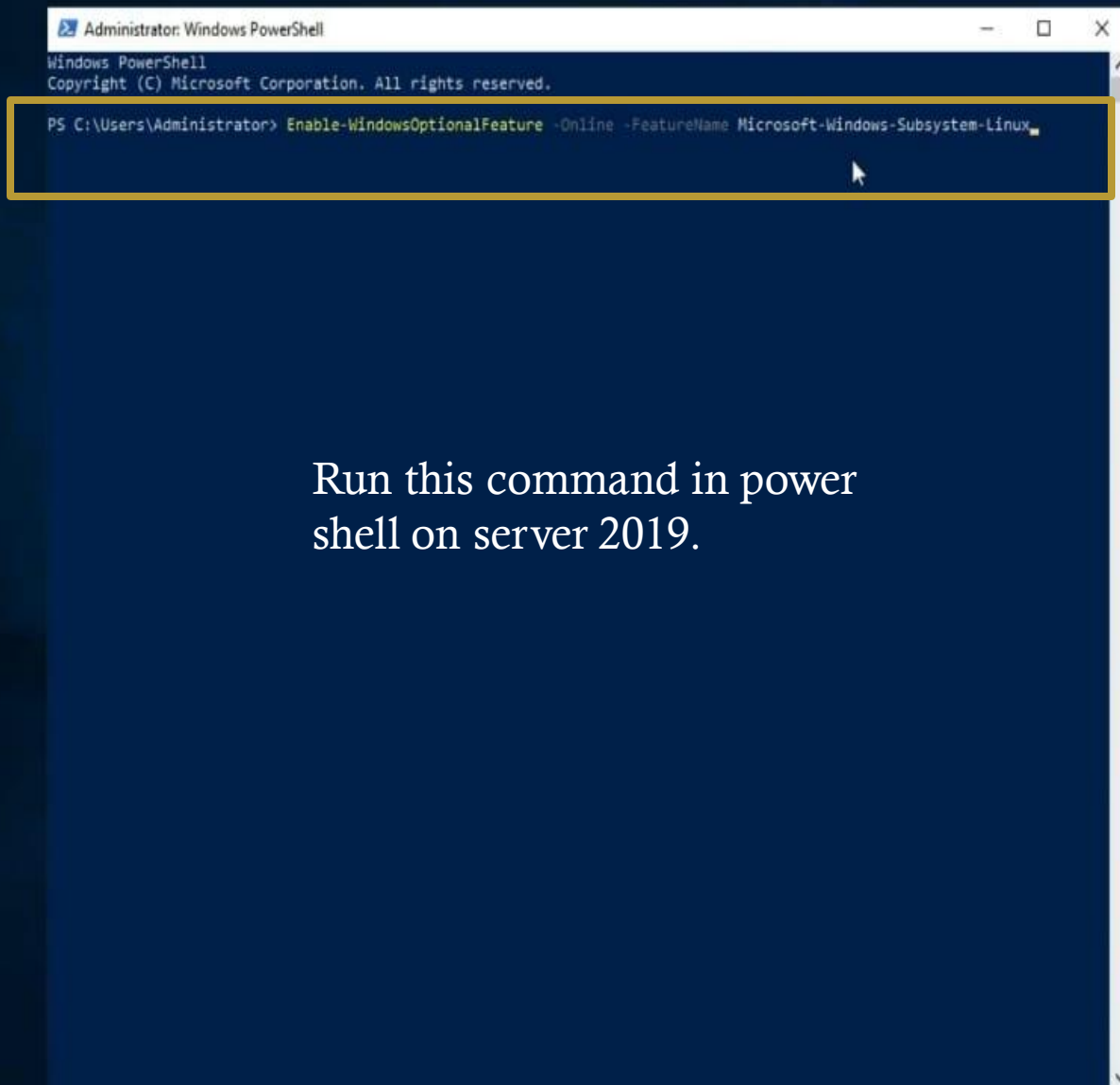
The general phases of the forensic process are: the identification of potential evidence; the acquisition of that evidence; analysis of the evidence; and production of a report.



You can go to the link > <https://bluecapesecurity.com/> > Free tutorials > Build your forensic workstation.

Setup for windows forensic

1. Download the virtualbox <https://www.virtualbox.org/wiki/Downloads> and download vhd iso 2019 <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019> and install the server 2019.
2. Start the powershell as a administrator and paste the command of the link `Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux` . And restart the server 2019.
3. Download the ubuntu iso file in this link <https://learn.microsoft.com/en-us/windows/wsl/install-manual#downloading-distributions>
4. Install ubuntu as a commandline in server 2019.
5. Install windows10 , open powershell as a administrator paste the command in this following link <https://learn.microsoft.com/en-us/windows/wsl/install-manual> and install ubuntu linux from Microsoft store.

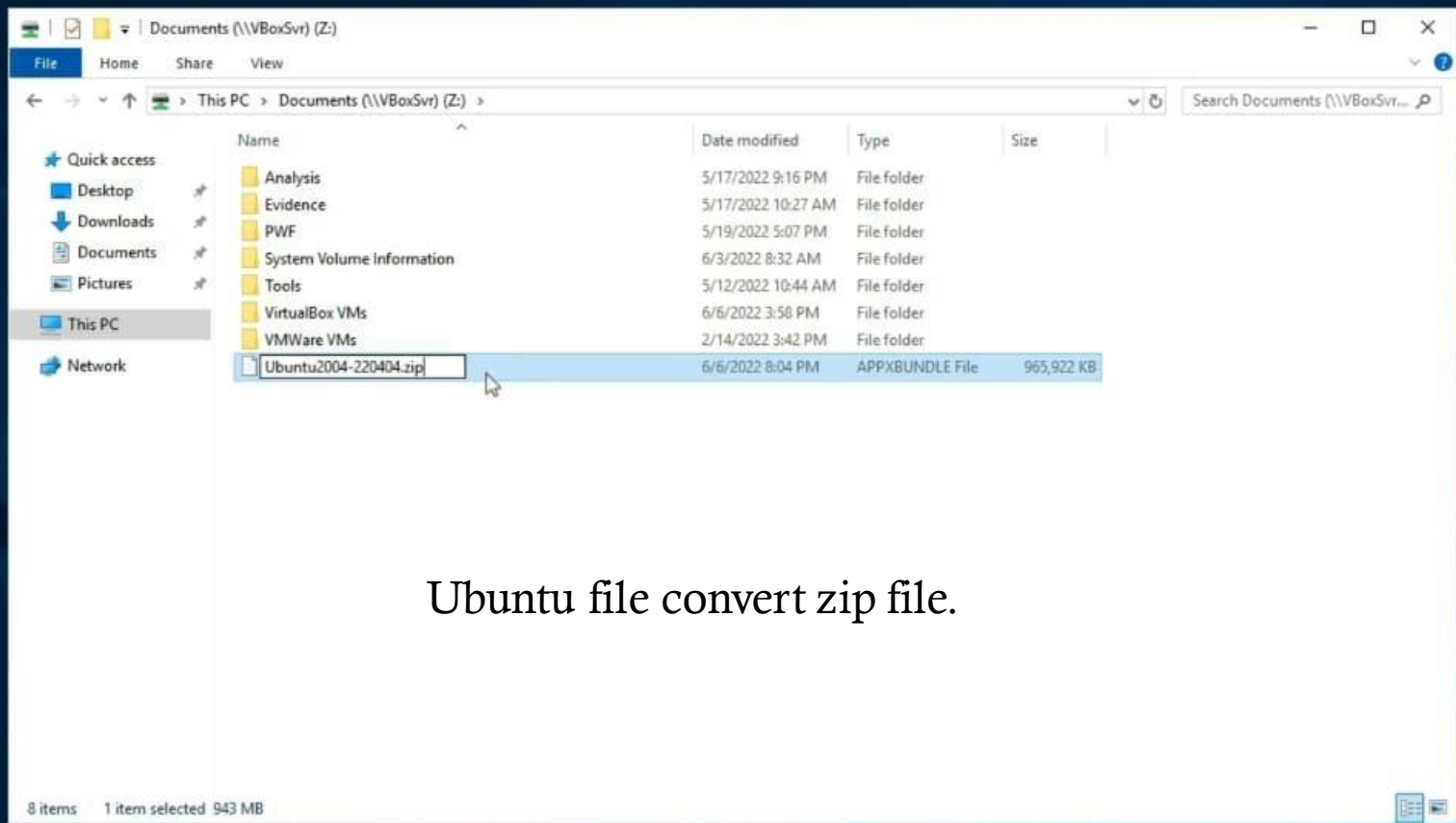


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux
```

Run this command in power shell on server 2019.



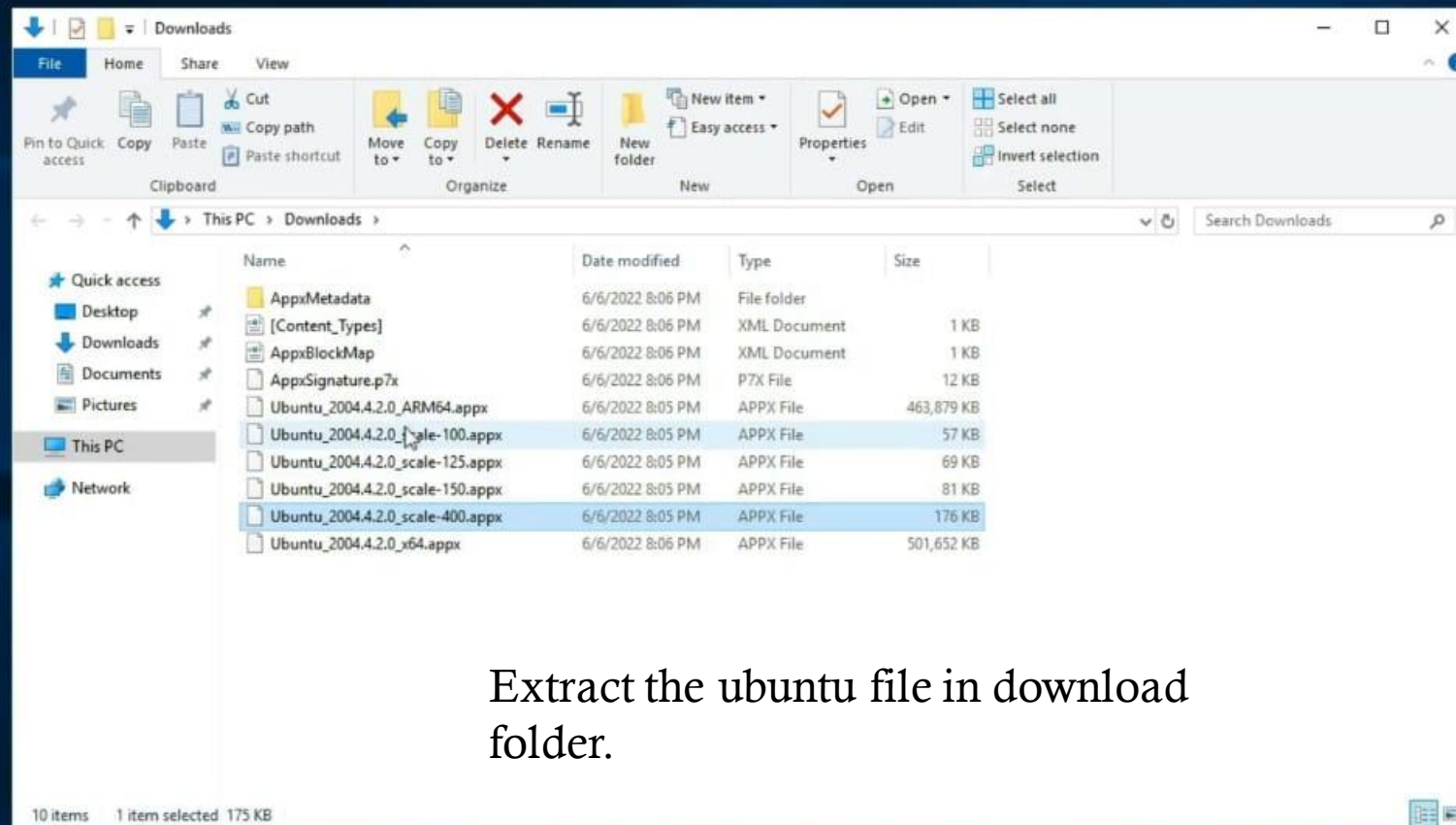


Ubuntu file convert zip file.

The screenshot shows a Windows File Explorer window titled "Documents (\\VBoxSvr) (Z:)" with the "Extract" ribbon tab active. The address bar shows the path "This PC > Documents (\\VBoxSvr) (Z:) >". The left sidebar shows "This PC" selected under "Network". The main pane displays a list of files and folders:

Name	Date modified	Type	Size
Analysis	5/17/2022 9:16 PM	File folder	
Evidence	5/17/2022 10:27 AM	File folder	
PWF	5/19/2022 5:07 PM	File folder	
System Volume Information	6/3/2022 8:32 AM	File folder	
Tools	5/12/2022 10:44 AM	File folder	
VirtualBox VMs	6/6/2022 3:58 PM	File folder	
VMWare VMs	2/14/2022 3:42 PM	File folder	
Ubuntu2004-220404	6/6/2022 8:04 PM	Compressed (zipp...	965,922 KB

At the bottom of the window, it shows "8 items" and "1 item selected 943 MB".



Extract the ubuntu file in download folder.

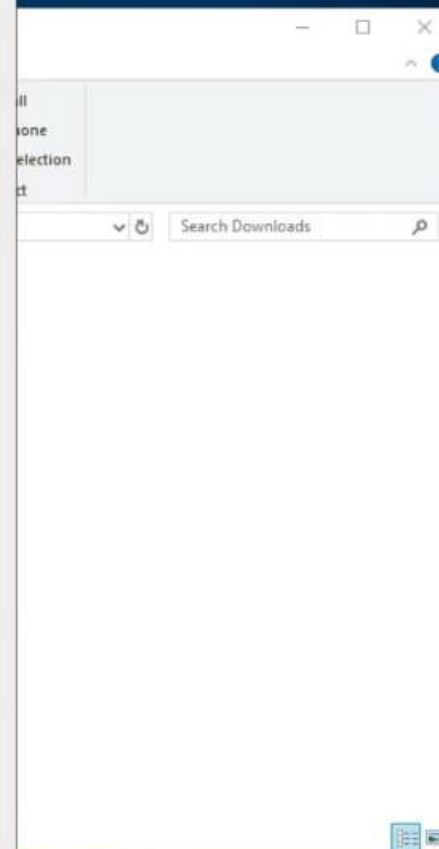

```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Downloads> dir

Directory: C:\Users\Administrator\Downloads

Mode                LastWriteTime         Length Name
----                -
d-----          6/6/2022  8:06 PM                AppxMetadata
-a----          6/6/2022  8:06 PM             338 AppxBlockMap.xml
-a----          6/6/2022  8:06 PM            11955 AppxSignature.p7x
-a----          6/6/2022  8:05 PM       475011248 Ubuntu_2004.4.2.0_ARM64.appx
-a----          6/6/2022  8:05 PM        58246 Ubuntu_2004.4.2.0_scale-100.appx
-a----          6/6/2022  8:05 PM        69891 Ubuntu_2004.4.2.0_scale-125.appx
-a----          6/6/2022  8:05 PM        81939 Ubuntu_2004.4.2.0_scale-150.appx
-a----          6/6/2022  8:05 PM       179710 Ubuntu_2004.4.2.0_scale-400.appx
-a----          6/6/2022  8:06 PM       513691210 Ubuntu_2004.4.2.0_x64.appx
-a----          6/6/2022  8:06 PM             469 [Content_Types].xml

PS C:\Users\Administrator\Downloads> Add-AppxPackage .\Ubuntu_2004.4.2.0_x64.appx
```

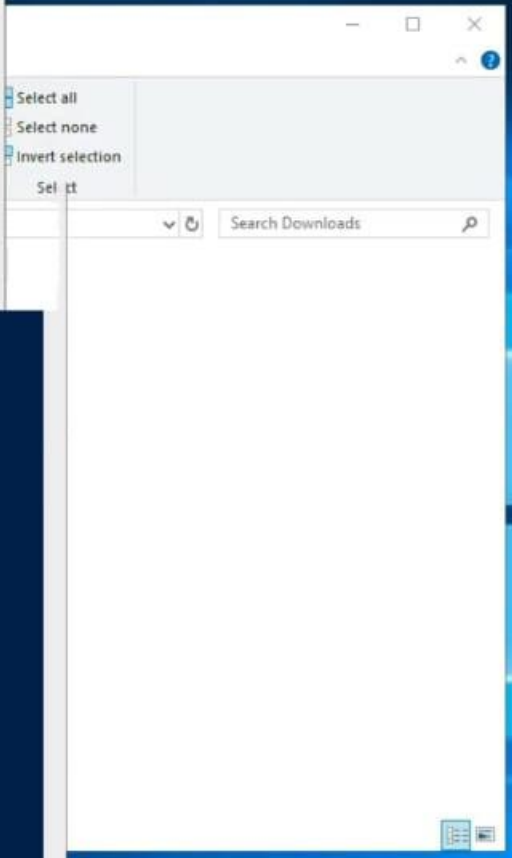
Open the power shell and run this command then after ubuntu installation will be start.



```
Ubuntu
Installing, this may take a few minutes...

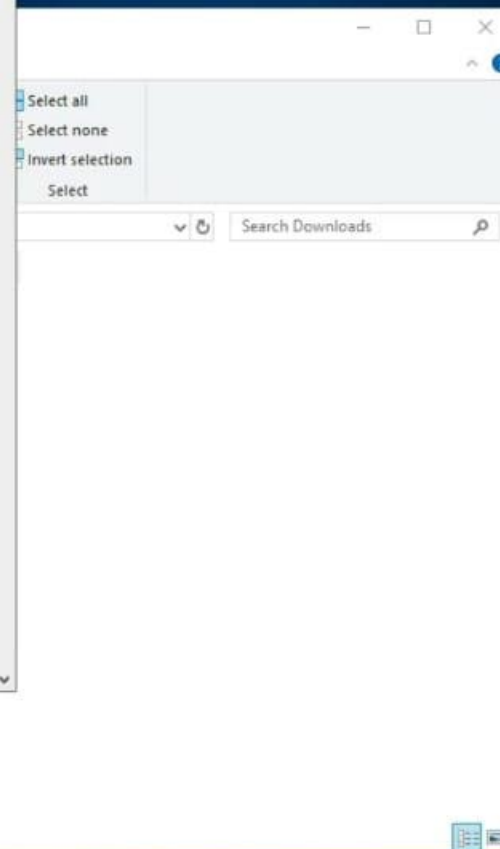
Please create a default UNIX user account. The username does not need to match your Windows username.
For more information visit: https://aka.ms/wslusers
Enter new UNIX username: _
```

Create a username – forensic
Create a password –
Admin@123 (Any..)



```
forensics@WIN-NVK3792LF90: ~  
Retype new password:  
passwd: password updated successfully  
Installation successful!  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 4.4.0-17763-Microsoft x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Mon Jun  6 20:14:11 DST 2022  
  
System load:  0.52      Processes:      7  
Usage of /home: unknown  Users logged in:  0  
Memory usage: 33%      IPv4 address for eth0: 10.0.2.15  
Swap usage:   0%  
  
1 update can be applied immediately.  
To see these additional updates run: apt list --upgradable  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
This message is shown once a day. To disable it please create the  
/home/forensics/.hushlogin file.  
forensics@WIN-NVK3792LF90:~$
```

Ubuntu start in
server 2019.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

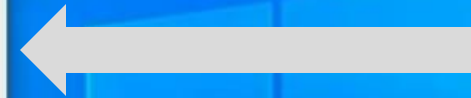
PS C:\Windows\system32> dism.exe /online /enable-feature /featurename:Microsoft-Windows-Subsystem-Linux /all /norestart

Deployment Image Servicing and Management tool
Version: 10.0.19041.844

Image Version: 10.0.19044.1288

Enabling feature(s)
[=====74.0%===== ]
```

Run this command in power shell on target machine.




Windows 10

Recycle

← Home Gaming Entertainment Productivity Deals

Search

✓ You own this app. **Install**




Ubuntu

Canonical Group Limited • Developer tools

★★★★☆ 81 [Share](#)

Install a complete Ubuntu terminal environment in minutes with Windows Subsystem for Linux (WSL). Develop cross-platform applications, improve your data science or web development workflows

More



[Overview](#) [System Requirements](#) [Reviews](#) [Related](#)

Available on

PC

Description

Install a complete Ubuntu terminal environment in minutes with Windows Subsystem for Linux (WSL). Develop cross-platform applications, improve your data science or web development workflows and manage IT infrastructure without leaving Windows.

Key features:

- Efficient command line utilities including bash, ssh, git, apt, npm, pip and many more

Install ubuntu in
Microsoft store

Recycle

← Home Gaming Entertainment Productivity Deals

Search

Ubuntu

```
Installing, this may take a few minutes...
Please create a default UNIX user account. The username does not need to match your Windows username.
For more information visit: https://aka.ms/wslusers
Enter new UNIX username: forensics
```

Create username and password.

Available on

PC

Description

Install a complete Ubuntu terminal environment in minutes with Windows Subsystem for Linux (WSL). Develop cross-platform applications, improve your data science or web development workflows and manage IT infrastructure without leaving Windows.

Key features:

- Efficient command line utilities including bash, ssh, git, apt, npm, pip and many more



6. Open server 2019 and change the following setting.

setting > date and time setting > select (UTC) Coordinated Universal time.

Go to the c drive and create a two folder Cases and Tools.

setting > virus and threat protection off > cloud-delivered protection off > Exclusion – Add click and select cases and tools folder one by one. And create a snapshot.

7. Install the tools in server 2019 for windows Forensic.

1. Download the Arsenal Image Mounter- <https://arsenalrecon.com/downloads>

2. Download the KAPE Tool- <https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape>

3. Download the Eric Zimmerman Tools - <https://ericzimmerman.github.io/#index.md>

4. Download the Regripper tool - <https://github.com/keydet89/RegRipper3.0>

5. Download the event log explorer – <https://eventlogxp.com/>

6. Download Notepad++ - <https://notepad-plus-plus.org/downloads/>

All tool copy in c drive Tools folder.

Install the setup of Event log and Notepad++.

Go to the C:/Tools/Get Zimmer tools > open powershell > .\Get-ZimmermanTools.ps1 –
Netversion 4.

```
Administrator: Windows PowerShell
PS C:\Tools\EZTools> .\Get-ZimmermanTools.ps1 -NetVersion 4

this script will discover and download all available programs
from https://ericzimmerman.github.io and download them to C:\Tools\EZTools

A file will also be created in C:\Tools\EZTools that tracks the SHA-1 of each file,
so rerunning the script will only download new versions.

To redownload, remove lines from or delete the CSV file created under C:\Tools\EZTools and rerun. Enjoy!

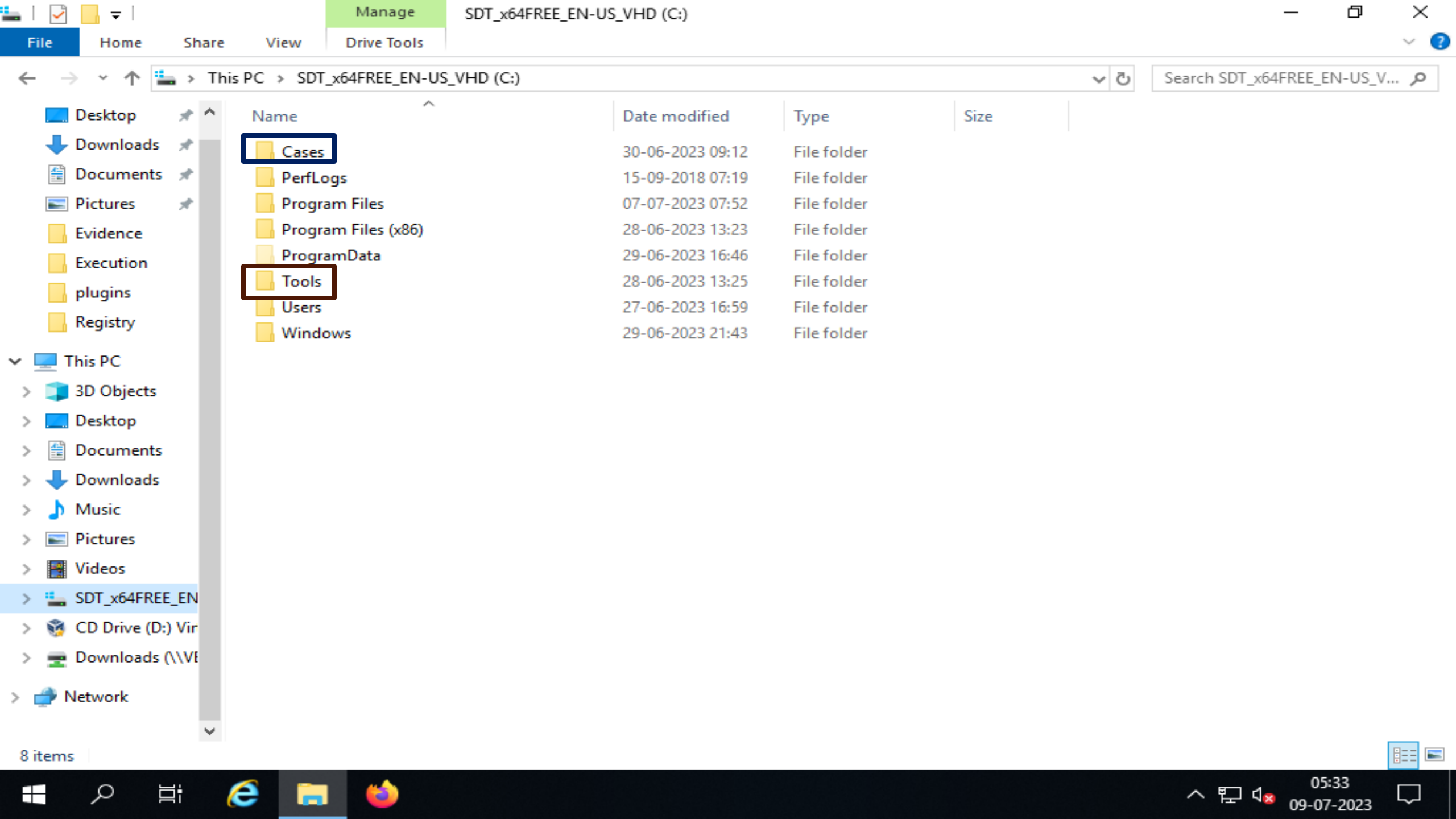
Use -NetVersion to control which version of the software you get (4 or 6). Default is getting both versions.

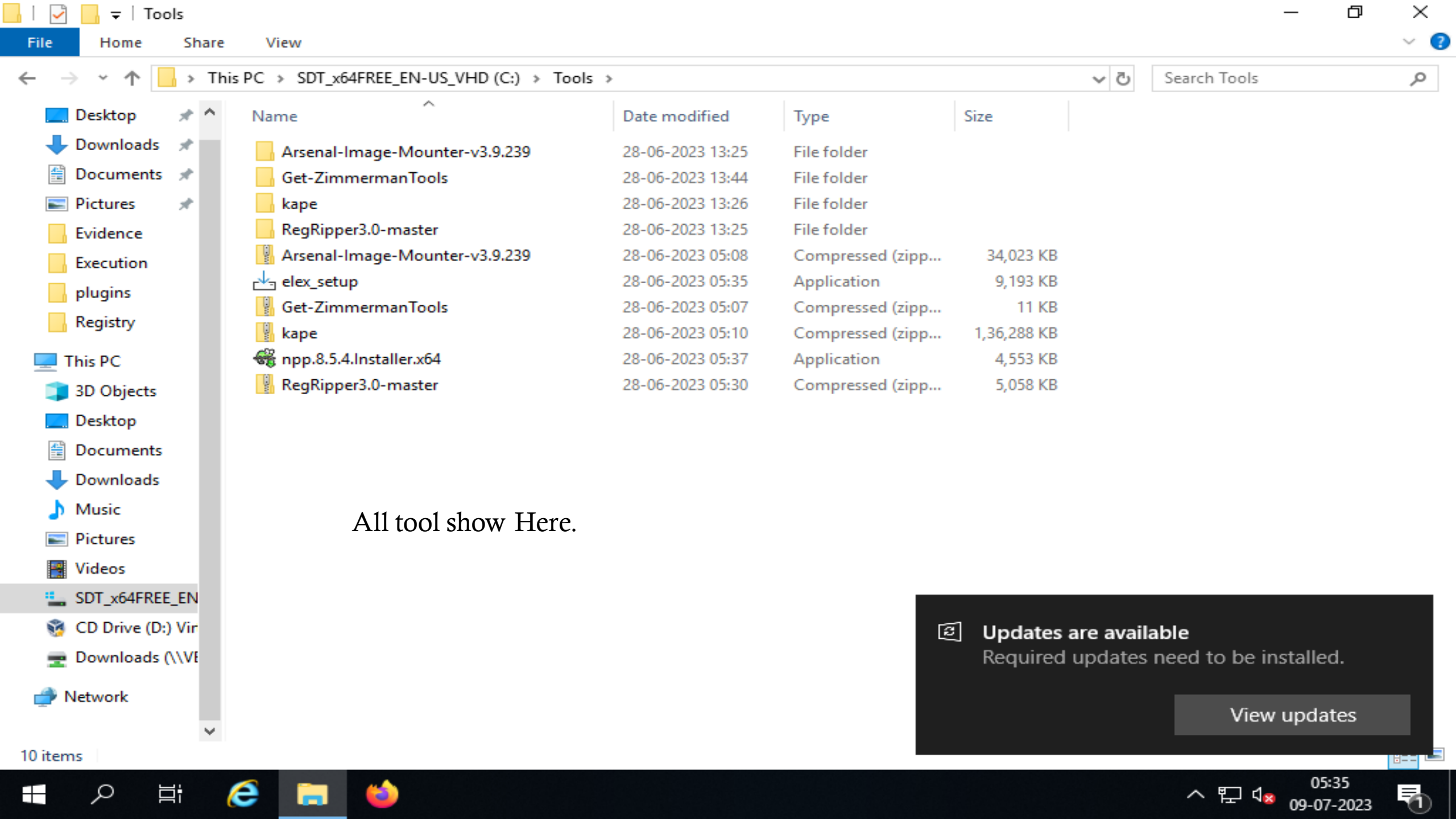
* Getting available programs...
* Files to download: 31
* Downloaded Get-ZimmermanTools.zip (Size: 15,158)
* Downloaded AmcacheParser.zip (Size: 4,403,385)
* Downloaded AppCompatCacheParser.zip (Size: 4,358,362)
* Downloaded bstrings.zip (Size: 3,664,596)
* Downloaded EvtXCmd.zip (Size: 5,278,734)
* Downloaded EZViewer.zip (Size: 73,114,127)
* Downloaded hasher.zip (Size: 51,299,411)
* Downloaded JLLCmd.zip (Size: 4,160,098)
* Downloaded JumpListExplorer.zip (Size: 56,040,986)
* Downloaded LECmd.zip (Size: 4,571,359)
* Downloaded MFTECmd.zip (Size: 4,214,450)
* Downloaded MFTEExplorer.zip (Size: 56,560,655)
* Downloaded PECmd.zip (Size: 3,690,100)
* Downloaded RBCmd.zip (Size: 3,298,635)
* Downloaded RecentFileCacheParser.zip (Size: 3,189,552)
* Downloaded RECcmd.zip (Size: 5,019,247)
* Downloaded RegistryExplorer.zip (Size: 64,705,900)
* Downloaded rla.zip (Size: 4,126,404)
* Downloaded SDBExplorer.zip (Size: 64,787,575)
* Downloaded SBECmd.zip (Size: 4,486,677)
* Downloaded ShellBagsExplorer.zip (Size: 77,989,497)
* Downloaded SQLECmd.zip (Size: 6,838,917)
* Downloaded SrumECmd.zip (Size: 4,365,882)
* Downloaded SumECmd.zip (Size: 3,603,159)
* Downloaded TimelineExplorer.zip (Size: 63,456,641)
* Downloaded VSCMount.zip (Size: 3,177,299)
* Downloaded WxTCmd.zip (Size: 4,141,090)
* Downloaded TlsGeolocate.zip (Size: 38,438,180)
* Downloaded TimeApp.zip (Size: 182,347)
* Downloaded XWFIM.zip (Size: 62,755,806)
* Downloaded ChangeLog.txt (Size: 31,572)

* Saving downloaded version information to C:\Tools\EZTools\!!!RemoteFileDetails.csv
PS C:\Tools\EZTools>
```

Using this command
all tool install in Eric
Zimmerman tool

modified	Type	Size
2022 11:36 PM	File folder	
2022 11:37 PM	File folder	
2022 11:37 PM	File folder	
2022 11:38 PM	File folder	
2022 11:37 PM	File folder	
2022 11:37 PM	File folder	
2022 11:37 PM	File folder	
2022 11:38 PM	File folder	
2022 11:37 PM	File folder	
2022 11:38 PM	File folder	
2022 11:38 PM	File folder	
2022 11:38 PM	File folder	
2022 11:38 PM	File folder	
2022 11:39 PM	File folder	
2022 11:39 PM	CSV File	5 KB
2022 12:30 PM	Application	4,548 KB
2022 11:28 AM	Application	4,417 KB
2022 12:31 PM	Application	3,994 KB
2022 11:39 PM	Text Document	31 KB
2022 10:58 PM	Windows PowerS...	32 KB





- Desktop
- Downloads
- Documents
- Pictures
- Evidence
- Execution
- plugins
- Registry
- This PC
- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- SDT_x64FREE_EN
- CD Drive (D:) Vir
- Downloads (\\V
- Network

Name	Date modified	Type	Size
Arsenal-Image-Mounter-v3.9.239	28-06-2023 13:25	File folder	
Get-ZimmermanTools	28-06-2023 13:44	File folder	
kape	28-06-2023 13:26	File folder	
RegRipper3.0-master	28-06-2023 13:25	File folder	
Arsenal-Image-Mounter-v3.9.239	28-06-2023 05:08	Compressed (zipp...	34,023 KB
elex_setup	28-06-2023 05:35	Application	9,193 KB
Get-ZimmermanTools	28-06-2023 05:07	Compressed (zipp...	11 KB
kape	28-06-2023 05:10	Compressed (zipp...	1,36,288 KB
npp.8.5.4.Installer.x64	28-06-2023 05:37	Application	4,553 KB
RegRipper3.0-master	28-06-2023 05:30	Compressed (zipp...	5,058 KB

All tool show Here.

Updates are available
Required updates need to be installed.

[View updates](#)

8. Install the windows 10 Enterprise version as a Target System and create a snapshot. <https://bluecapesecurity.com/prepare-your-target-system/>

Go to the setting > Windows Update > Advance option > Update off.

Virus and threat protection > manage setting > Real-time protection off and Cloud delivered protection off.

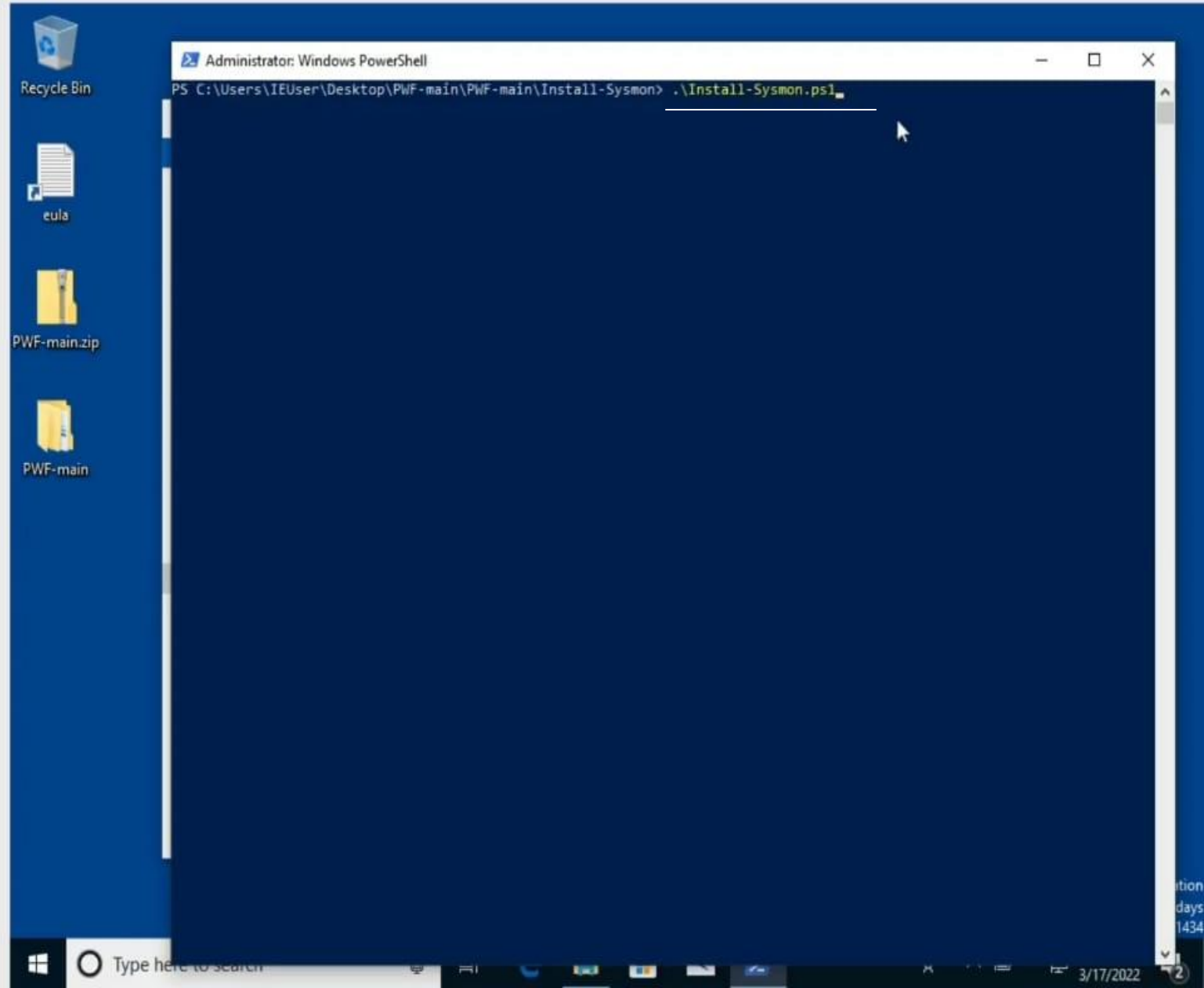
Attack Script Preparation - Go to the url <https://github.com/bluecapesecurity/PWF> zip file download and extract file.

2 script is execute here.

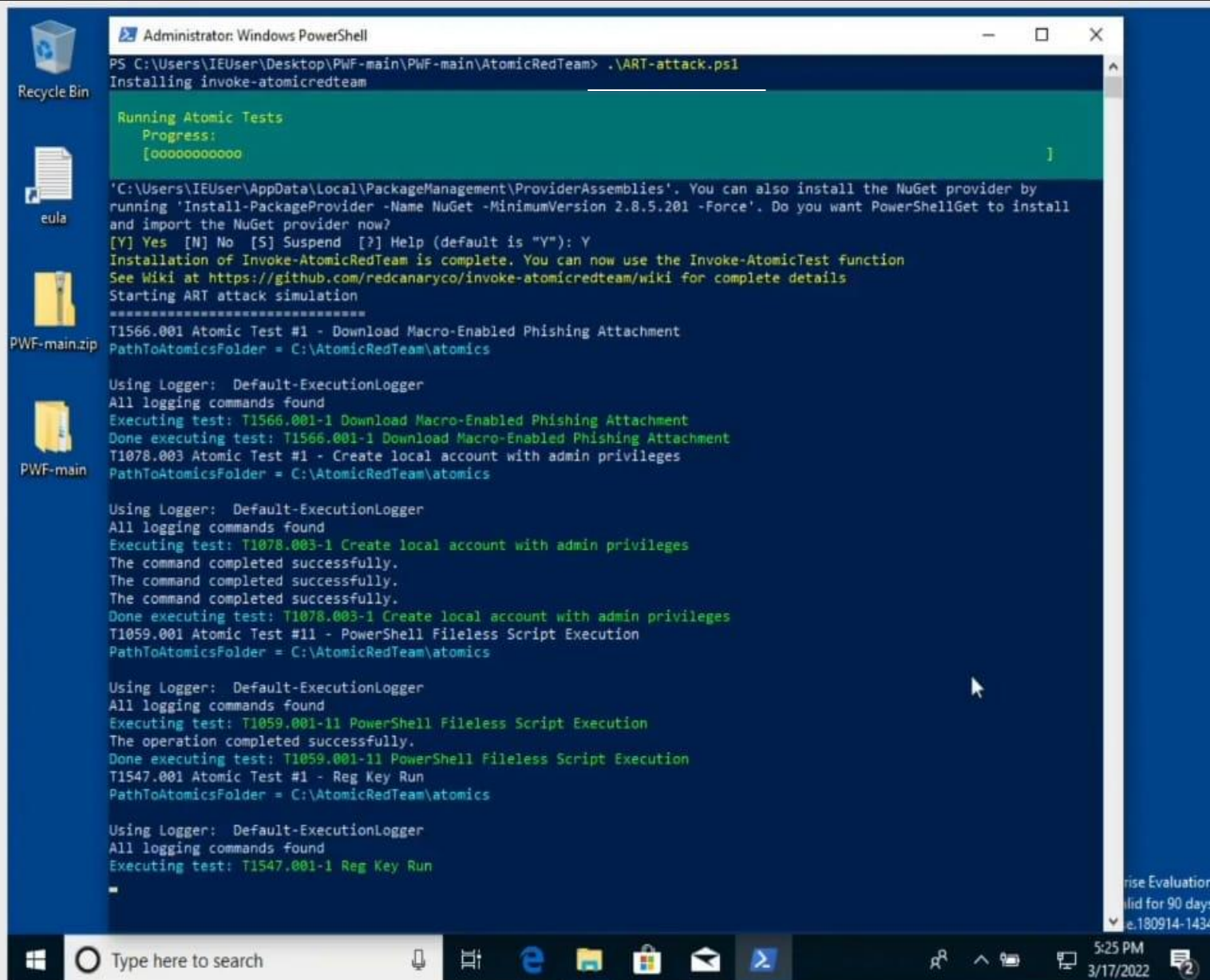
1. **Sysmon script** – C:\users\denisha\Desktop\PWF-main\PWF-main/Install-Sysmon > powershell as administrator > .\Install-sysmon.ps1.

2. **ART Attack script** - C:\users\denisha\Desktop\PWF-main\PWF-main\AtomicRedTeam > open powershell as Administrator > .\ART-attack.ps1.

Sysmon Script Run



ART Attack Script



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt shows the execution of the script `.\ART-attack.ps1` in the directory `C:\Users\IEUser\Desktop\PWF-main\AtomicRedTeam`. The output includes a progress bar for "Running Atomic Tests", a confirmation prompt for installing the NuGet provider, and the start of the ART attack simulation. The simulation begins with "T1566.001 Atomic Test #1 - Download Macro-Enabled Phishing Attachment".

```
Administrator: Windows PowerShell
PS C:\Users\IEUser\Desktop\PWF-main\AtomicRedTeam> .\ART-attack.ps1
Installing invoke-atomicredteam

Running Atomic Tests
Progress:
[oooooooooooo]

'C:\Users\IEUser\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function
See Wiki at https://github.com/redcanaryco/invoke-atomicredteam/wiki for complete details
Starting ART attack simulation
=====
T1566.001 Atomic Test #1 - Download Macro-Enabled Phishing Attachment
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Using Logger: Default-ExecutionLogger
All logging commands found
Executing test: T1566.001-1 Download Macro-Enabled Phishing Attachment
Done executing test: T1566.001-1 Download Macro-Enabled Phishing Attachment
T1078.003 Atomic Test #1 - Create local account with admin privileges
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Using Logger: Default-ExecutionLogger
All logging commands found
Executing test: T1078.003-1 Create local account with admin privileges
The command completed successfully.
The command completed successfully.
The command completed successfully.
Done executing test: T1078.003-1 Create local account with admin privileges
T1059.001 Atomic Test #11 - PowerShell Fileless Script Execution
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Using Logger: Default-ExecutionLogger
All logging commands found
Executing test: T1059.001-11 PowerShell Fileless Script Execution
The operation completed successfully.
Done executing test: T1059.001-11 PowerShell Fileless Script Execution
T1547.001 Atomic Test #1 - Reg Key Run
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Using Logger: Default-ExecutionLogger
All logging commands found
Executing test: T1547.001-1 Reg Key Run
-
```

Free Evaluation
Valid for 90 days
e.180914-1434

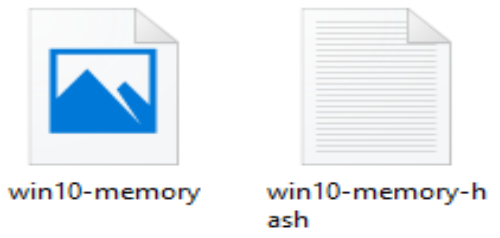
Data Collection

9.Memory Acquisition of the target system

Step for Memory Acquisition :

1. Create a Evidence Folder in Main PC.
2. Go to C:\Users\Documents\Evidence > open cmd > “C:\program Files\Oracle\Virtual Box\VBoxManage.exe”
3. SET PATH=%PATH%;”C:\Programs Files\Oracle\Virtual Box”
4. vboxmanage.exe
5. vboxmanage list vms
6. VBoxmanage debugvm id paste machine(target machine) dumpvm core –filename win10-memory.raw
7. Certutil –hashfile win10-memory.raw > win10.memory –hash.txt.

- ★ Quick access
 - Desktop
 - Downloads
 - Documents
 - Pictures
 - 3) Setting up your forensic
 - 28
 - 30
 - Screenshots
- OneDrive
- This PC
 - Desktop
 - Documents
 - Downloads
 - Music
 - Pictures
 - Videos
 - New Volume (C:)
 - USB Drive (D:)
 - New Volume (F:)
 - USB Drive (D:)
 - Network



10. Disk Acquisition target system

The screenshot displays the Oracle VM VirtualBox Manager interface. On the left, three virtual machines are listed: 'win2019-for (34 practical)' (Running), 'windows 10 (fresh installation)' (Powered Off), and 'Target system (After attack shutdown)' (Powered Off). The main pane shows the 'Hard disks' tab for the 'Target system' VM. A table lists the disks, with 'Target system.vdi' selected. A context menu is open over this disk, showing options like 'Copy...', 'Move...', 'Remove...', 'Release...', 'Search', and 'Properties'. The 'Attributes' pane at the bottom shows the disk's type as 'Normal', its location, and a size slider set to 50.00 GB.

Name	Virtual Size	Actual Size
{0926ccea-dfd7-4e08-bd93-7a85bd797974}_copy.vhd	--	--
> 17763.737.amd64fre.rs5_release_svc_refresh.190906-2324_server_serverdatacente...	40.00 GB	8.31 GB
Target system.vdi	50.00 GB	50.00 GB
> {0e92291a-4319-4be6-8d4f-c9213ea20f88}.vdi	50.00 GB	1.09 GB
{ab...}.vdi	50.00 GB	4.69 GB
{cabe...}.vdi	50.00 GB	9.42 GB
{...}.vdi	50.00 GB	1.36 GB
> window...	50.00 GB	50.00 GB
> win...	--	--

Attributes Information

Type: Normal

Location: C:\Users\Denisha\VirtualBox VMs\Target system\Snapshots\{0e92291a-4319-4be6-8d4f-c9213ea20f88}.vdi

Description:

Size: 50.00 GB

4.00 MB 2.00 TB

Apply Reset



Type here to search



11:54

09-07-2023





Tools



Add



Create



Copy



Move



Remove



Release



Search



Properties



Refresh



Refresh



win2019-for (34 practical)

Running



windows 10 (fresh installation)

Powered Off



Target system (After attack)

Powered Off

Hard disks

Optical disks

Floppy disks

Name

{0926ccea-dfd7-4e08-bd93-7a85bd797974}_copy.vhd

Virtual Size

Actual Size

--	--
40.00 GB	8.31 GB
50.00 GB	50.00 GB
50.00 GB	1.09 GB
50.00 GB	4.69 GB
50.00 GB	9.42 GB
50.00 GB	1.36 GB
50.00 GB	50.00 GB
--	--

Copy Virtual Disk



Virtual Hard disk file type

Please choose the type of file that you would like to use for the destination virtual disk image. If you do not need to use it with other virtualization software you can leave this setting unchanged.

- VDI (VirtualBox Disk Image)
- VHD (Virtual Hard Disk) ←
- VMDK (Virtual Machine Disk)

Expert Mode

Back

Next

Cancel

Location: C:\Users\Denisha\VirtualBox VMs\Target system\Snapshots\{0e92291a-4319-4be6-8d4f-c9213ea20f88}.vdi

Description:

Size:

4.00 MB

2.00 TB

50.00 GB

Apply

Reset



Type here to search



11:54

09-07-2023





win2019-for (34 practical)
Running

windows 10 (fresh installation)
Powered Off

Target system (After attack)
Powered Off

Hard disks Optical disks Floppy disks

Name	Virtual Size	Actual Size
{0926ccea-dfd7-4e08-bd93-7a85bd797974}_copy.vhd	--	--
atacente...	40.00 GB	8.31 GB
	50.00 GB	50.00 GB
	50.00 GB	1.09 GB
	50.00 GB	4.69 GB
	50.00 GB	9.42 GB
	50.00 GB	1.36 GB
	50.00 GB	50.00 GB
	--	--

Copy Virtual Disk

Storage on physical hard disk

Please choose whether the new virtual disk image file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** disk image file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** disk image file may take longer to create on some systems but is often faster to use.

Pre-allocate Full Size
 Split into 2GB parts

Back **Next** Cancel

Location:

Description:

Size: 50.00 GB

4.00 MB 2.00 TB

Apply Reset



Type here to search





Tools



Add



Create



Copy



Move



Remove



Release



Search



Properties



Refresh



win2019-for (34 practical)

Running



windows 10 (fresh installation)

Powered Off



Target system (After attack)

Powered Off

Hard disks

Optical disks

Floppy disks

Name

! {0926ccea-dfd7-4e08-bd93-7a85bd797974}_copy.vhd

Virtual Size


Actual Size

--	--
40.00 GB	8.31 GB
50.00 GB	50.00 GB
50.00 GB	1.09 GB
50.00 GB	4.69 GB
50.00 GB	9.42 GB
50.00 GB	1.36 GB
50.00 GB	50.00 GB
--	--

Copy Virtual Disk

Location and size of the disk image

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.



Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

50.00 GB 2.00 TB

Back

Finish

Cancel

Location: C:\Users\Denisha\VirtualBox VMs\Target system\Snapshots\{0e92291a-4319-4be6-8d4f-c9213ea20f88}.vdi

Description:

Size:

4.00 MB

2.00 TB

Apply

Reset



Type here to search

11:55
09-07-2023

Data Examination

Mounting the disk Image with Arsenal Image Mounter

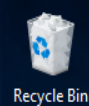
You can enter the Target system harddisk



File Explorer window showing the 'Tools' folder in 'SDT_x64FREE_EN-US_VHD (C:)'. The file 'Arsenal-Image-Mounter-v3.9.239' is highlighted.

Name	Date modified	Type	Size
Arsenal-Image-Mounter-v3.9.239	28-06-2023 13:25	File folder	
Get-ZimmermanTools	28-06-2023 13:44	File folder	
kape	28-06-2023 13:26	File folder	
RegRipper3.0-master	28-06-2023 13:25	File folder	
Arsenal-Image-Mounter-v3.9.239	28-06-2023 05:08	Compressed (zipp...	34,023 KB
elex_setup	28-06-2023 05:35	Application	9,193 KB
Get-ZimmermanTools	28-06-2023 05:07	Compressed (zipp...	11 KB
kape	28-06-2023 05:10	Compressed (zipp...	1,36,288 KB
npp.8.5.4.Installer.x64	28-06-2023 05:37	Application	4,553 KB
RegRipper3.0-master	28-06-2023 05:30	Compressed (zipp...	5,058 KB

Open image mounter.



File Explorer window showing the contents of the 'Arsenal-Image-Mounter-v3.9.239' folder. The file 'ArsenalImageMounter' is highlighted.

Name	Date modified	Type	Size
lib	02-06-2022 10:50	File folder	
runtimes	21-11-2022 20:48	File folder	
aim_cli	27-08-2022 20:45	File	1 KB
aim_cli.dll	28-02-2023 17:02	Application extens...	53 KB
aim_cli	28-02-2023 17:03	Application	114 KB
aim_cli.runtimeconfig.json	26-11-2022 16:01	JSON File	1 KB
Arsenal Recon - End User License Agree...	10-08-2022 06:16	Text Document	28 KB
ArsenalImageMounter.dll	28-02-2023 17:03	Application extens...	521 KB
ArsenalImageMounter.Forms.dll	28-02-2023 17:03	Application extens...	43 KB
ArsenalImageMounter.deps.json	28-02-2023 17:02	JSON File	73 KB
ArsenalImageMounter.dll	28-02-2023 17:02	Application extens...	20,427 KB
ArsenalImageMounter	28-02-2023 17:02	Application	494 KB
ArsenalImageMounter	29-06-2023 16:54	Text Document	1 KB
ArsenalImageMounter.runtimeconfig.json	28-02-2023 17:02	JSON File	1 KB
DiscUtils.BootConfig.dll	28-02-2023 17:03	Application extens...	52 KB
DiscUtils.Btrfs.dll	28-02-2023 17:03	Application extens...	67 KB
DiscUtils.Core.dll	28-02-2023 17:03	Application extens...	263 KB
DiscUtils.Dmg.dll	28-02-2023 17:03	Application extens...	41 KB
DiscUtils.Ext.dll	28-02-2023 17:03	Application extens...	52 KB
DiscUtils.Fat.dll	28-02-2023 17:03	Application extens...	84 KB
DiscUtils.HfsPlus.dll	28-02-2023 17:03	Application extens...	58 KB



Recycle Bin



Firefox




Event Log Explorer



Notepad++

Manage Arsenal-Image-Mounter-v3.9.239

ARSENAL IMAGE MOUNTER ver 3.9.239
Brought to you by the developers of [Registry Recon](#)



ARSENAL RECON

Arsenal Image Mounter source code and APIs are available for royalty-free use by open source projects. **Commercial projects must obtain alternative licensing.** Contact [Arsenal Recon](#) for more information.

No License Detected - Free Mode Enabled

Arsenal Image Mounter is currently running in Free Mode which supports basic mounting of various disk image formats. For additional functionality, including mounting Volume Shadow Copies and launching virtual machines, please [upgrade to Professional Mode](#).

For digital forensics consulting services, contact [Arsenal Consulting](#).

Disclaimer

Arsenal Image Mounter ("the Software") is provided "AS IS" and "WITH ALL FAULTS," without warranty of any kind, including without limitation the warranties of merchantability, fitness for a particular purpose and non-infringement. Arsenal Consulting, Inc. (d/b/a "Arsenal Recon") makes no warranty that the Software is free of defects or is suitable for any particular purpose. In no event shall Arsenal Consulting, Inc. be responsible for loss or damages arising from the installation or use of the Software, including but not limited to any indirect, punitive, special, incidental or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses. The entire risk as to the quality and performance of the Software is borne by you. Should the Software prove defective, you and not Arsenal Consulting, Inc. assume the entire cost of any service and repair.

OK Enter license Acknowledgments

53 items | 1 item selected 493 KB | 28-02-2023 17:04 | Application extens 280 KB

Windows Server 2019 Datacenter Evaluation
 Windows License valid for 178 days
 Build 17763.rs5_release.180914-1434

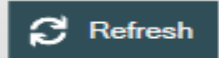
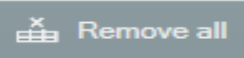
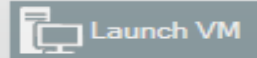
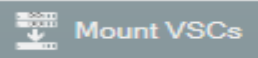
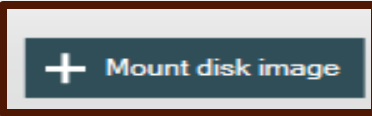


Recycle Bin

Arsenal Image Mounter v3.0.330

Arsenal Image Mounter

File BitLocker Advanced Help



ARSENAL RECON

53 items | 1 item selected 493 KB | D:\c\file Nffc.dll | 28-02-2023 17:04 | Application extens | 280 KB

Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434



17:03
29-06-2023



Recycle Bin

Arsenal Image Mounter v2.0.220

Arsenal Image Mounter

Mount image file

« Downloads (\...\ > Evidence Search Evidence

Organize New folder

Name	Date modified	Type
{0926ccea-dfd7-4e08-bd93-7a85bd79797...}	29-06-2023 15:38	Hard Disk
win10-memory.raw	29-06-2023 09:00	RAW File

Select the disk of target machine

File name: {0926ccea-dfd7-4e08-bd93-7a85b... Supported formats

Open Cancel

+ Mount disk image Mount VSCs Launch VM Remove Remove all Refresh

AR ARSENAL RECON

53 items 1 item selected 493 KB

Disk device, read only

Mount the disk image as a read-only disk device. No write operations will be allowed.

Disk device, write temporary

Mount the disk image as a writable disk device using the AIM write filter. Modifications will be written to a write-overlay differencing file and the original disk image will not be changed. Sometimes referred to as write-overlay or write-copy mode. (Note - required for launching virtual machines.)

Specify alternate differencing file location

Delete differencing file after unmount

Store differencing data in host RAM only (not in a file)

Windows file system driver bypass, read only

Mount the disk image as a virtual read-only file system, using DiscUtils rather than Windows file system drivers. This mount option is often used to bypass file system security, expose NTFS metafiles and streams, and recover deleted files. May also be useful to read files from disk images containing corrupted file systems. Please note, BitLocker-protected volumes are not supported and disk size values are an approximation of each volume's total file size (including things like multiple links to the same file and files with sparse allocation) so the size may appear larger than the expected volume size.

Disk device, write original

Mount the disk image as a writable disk device. Caution, modifications will be written to the original disk image.

Windows file system driver bypass, write original

Mount the disk image as a virtual writable file system. Caution, modifications will be written to the original disk image. This mount option bypasses file system security but does not expose most NTFS metafiles and streams.

Sector size:

Fake disk signature

Report a random disk signature to Windows. Useful if the disk image contains a zeroed-out disk signature or you are attempting to mount a duplicate disk signature. (Note - requires a valid MBR and partition table. Not compatible with GPT partitions or images without a partition table.)

Create "removable" disk device

Emulate the attachment of a USB thumb drive, which may facilitate the successful mounting of images containing partitions rather than complete disks or images without partition tables. (Caution - see relevant FAQ on our website for caveats.)

Automatically remount at Arsenal Image Mounter startup

OK

Cancel

The screenshot shows a Windows File Explorer window titled "Local Disk (F:)". The left sidebar shows the navigation pane with "Local Disk (F:)" selected. The main pane displays a list of folders with columns for Name, Date modified, Type, and Size.

Name	Date modified	Type	Size
AtomicRedTeam	28-06-2023 17:57	File folder	
PerfLogs	07-12-2019 09:14	File folder	
Program Files	28-06-2023 16:30	File folder	
Program Files (x86)	06-10-2021 13:58	File folder	
Users	28-06-2023 16:32	File folder	
Windows	29-06-2023 08:01	File folder	

Show the hard disk of Target system in Forensic Workstation and you can show all data.

Creating a triage data collection with KAPE Tool

The image shows the KAPE (Kali Automated Post-Exploitation) tool interface and a Windows File Explorer window. The KAPE tool is running in a terminal window, showing the command line: `.\kape.exe --tsource E: --tdest C:\Cases`. The File Explorer window shows the 'Targets' folder, which contains the following files and folders:

Name	Date modified	Type	Size
Documentation	3/19/2022 11:31 PM	File folder	
Modules	3/23/2022 9:58 PM	File folder	
Targets	3/23/2022 9:58 PM	File folder	
ChangeLog	Date created: 3/19/2022 11:31 PM	Text Document	21 KB
Get-System-Info.ps1	Size: 372 KB	Windows PowerShell Script	17 KB
gkape.exe	Folders: IDisabled, ILocal, Antivirus, Apps, Browsers, ...	Application	61,623 KB
gkape.settings	Files: CompoundTargetGuide.guide, ...	SETTINGS File	1 KB
kape.exe	3/23/2022 10:24 PM	Application	7,038 KB

Using kape tool store the permanent data of target system in forensic workstation.

All Data is store in Cases Folder.

File Tools

Use Target options

Target source: E:\

Target destination: C:\Cases

Flush Add %d Add %m

Targets (Double-click to edit a target)

Drag a column header here to group by that column

Selected	Name	Folder	Description
<input type="checkbox"/>	CombinedLogs	Compound	Collect Event logs, Trace I...
<input type="checkbox"/>	EventLogs	Windows	Event logs
<input type="checkbox"/>	EventLogs-RDP	Windows	Collect Win7+ RDP relate...
<input type="checkbox"/>	EventTraceLogs	Windows	Event Trace Logs
<input type="checkbox"/>	EventTranscriptDB	Win...	Kape Triage collections that will collect most of the files needed for a DFIR Investigation. This module pulls evidence from File System files, Registry Hives, Event Logs, Scheduled Tasks, Evidence of Execution, SRUM data, SUM data, Web Browser data (IE/Edge, Chrome, Mozilla history), and 3rd party software logs, 3rd party antivirus software logs, Windows 10 Timeline database, and \$! Recycle Bin data files.
<input type="checkbox"/>	KapeTriage	Con...	
<input type="checkbox"/>	MiniTimelineCollection	Compound	MPF, Registry and Event...

Process VSCs Deduplicate

Container: None VHDX VHD Zip

SHA-1 exclusions: []

Base name: []

Zip container Transfer

Target variables Transfer options

Target variables: []

Key: []

Value: []

Add

Use Module options

Module options

Module source: []

Module destination: []

Flush Add %d Add %m Zip

Modules (Double-click to edit a module)

Selected	Name	Folder	Category	Description
<input type="checkbox"/>	/ToolSync	Compound	Sync	Sync for new Maps, E...
<input type="checkbox"/>	IEParser	Compound	Modules	Eric Zimmerman Parser
<input type="checkbox"/>	AncacheParser	EZTools	ProgramExecution	AncacheParser: ext...
<input type="checkbox"/>	AppCompatCacheParser	EZTools	ProgramExecution	AppCompatCachePar...
<input type="checkbox"/>	bstings_AnonWallet	bstings	KeywordSearches	Use bstings to GREP...
<input type="checkbox"/>	bstings_BrowserHives	bstings	KeywordSearches	Use bstings to GREP...

Export format: Default CSV HTML JSON

Module variables: []

Key: []

Value: []

Add

Other options

Debug messages Trace messages Ignore FTK warning

Zip password: [] Retain local copies

Current command line

```
.\kape.exe --tsource E: --tdest C:\Cases --flush --gui
```

Copy command Sync with GitHub Execute

Documentation Targets available: 254 Targets selected: 0 Modules available: 253 Modules selected: 0 Disable flush warnings



File Tools

Use Target options

Target source: E:\

Target destination: C:\Cases Flush Add %d Add %m

Targets (Double-click to edit a target)

Drag a column header here to group by that column: event

Selected	Name	Folder	Description
<input type="checkbox"/>	CombinedLogs	Compound	Collect Event logs, Trace I...
<input type="checkbox"/>	EventLogs	Windows	Event logs
<input type="checkbox"/>	EventLogs-RDP	Windows	Collect Win7+ RDP relate...
<input type="checkbox"/>	EventTraceLogs	Windows	Event Trace Logs
<input type="checkbox"/>	EventTranscriptDB		
<input checked="" type="checkbox"/>	KapeTriage		
<input type="checkbox"/>	MiniTimelineCollection		

Process VSCs Deduplicate

SHA-1 exclusions

Target variables Transfer options

Target variables

Value

Use Module options

Module options

Module source

Module destination

Flush Add %d Add %m Zip

Modules (Double-click to edit a module)

Drag a column header here to group by that column:

Selected	Name	Folder	Category	Description
<input type="checkbox"/>	IToolSync	Compound	Sync	Sync for new Maps, B...
<input type="checkbox"/>	IEDParser	Compound	Modules	Eric Zimmerman Parser...
<input type="checkbox"/>	AmcacheParser	EZTools	ProgramExecution	AmcacheParser: extr...
<input type="checkbox"/>	AppCompatCacheParser	EZTools	ProgramExecution	AppCompatCachePar...
<input type="checkbox"/>	Remote Access			BMC-Tools: RDP Bitn...
<input type="checkbox"/>	Modules			Run all bitstrings Modu...
<input type="checkbox"/>	KeywordSearches			Use bitstrings to GREP
<input type="checkbox"/>	KeywordSearches			Use bitstrings to GREP

Key

Value

Other options

Debug messages Trace messages Ignore FTK warning

Zip password

Retain local copies

Current command line

```
.\kape.exe --tsource E: --tdest C:\Cases --tflush --target KapeTriage --ifw --gui
```

Documentation Targets available: 254 Targets selected: 1 Modules available: 253 Modules selected: 0 Disable flush warnings

DATA DESTRUCTION WARNING!

!!! WARNING !!!

One or more flush options are enabled!

This means that the contents of 'Target destination' and/or 'Module destination' will be DELETED prior to KAPE running!

Click 'OK' to continue or 'Cancel' to abort.



Select Total execution time: 115.0162 seconds

```

Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!
Found 675 files in 10.536 seconds. Beginning copy...
Deferring 'E:\$MFT' due to UnauthorizedAccessException...
Deferring 'E:\$LogFile' due to UnauthorizedAccessException...
Deferring 'E:\$Extend\$UsnJrnl:$J' due to NotSupportedException...
Deferring 'E:\$Extend\$UsnJrnl:$Max' due to NotSupportedException...
Deferring 'E:\$Secure:$SDS' due to NotSupportedException...
Deferring 'E:\$Boot' due to UnauthorizedAccessException...
Deferring 'E:\$Extend\$RmMetadata\$TxflLog\$Tops:$T' due to NotSupportedException...
Deferred file count: 7. Copying locked files...
Copied deferred file 'E:\$MFT' to 'C:\Cases\E\$MFT'. Hashing source file...
Copied deferred file 'E:\$LogFile' to 'C:\Cases\E\$LogFile'. Hashing source file...
Skipping sparse data area in $J!
Copied deferred file 'E:\$Extend\$UsnJrnl:$J' to 'C:\Cases\E\$Extend\$J'. Hashing source file...
Copied deferred file 'E:\$Extend\$UsnJrnl:$Max' to 'C:\Cases\E\$Extend\$Max'. Hashing source file...
Copied deferred file 'E:\$Secure:$SDS' to 'C:\Cases\E\$Secure_$SDS'. Hashing source file...
Copied deferred file 'E:\$Boot' to 'C:\Cases\E\$Boot'. Hashing source file...
Copied deferred file 'E:\$Extend\$RmMetadata\$TxflLog\$Tops:$T' to 'C:\Cases\E\$Extend\$RmMetadata\$TxflLog\$T'. Hashing source file...

Copied 601 (Deduplicated: 74) out of 675 files in 114.9477 seconds. See '*_CopyLog.csv' in 'C:\Cases' for copy details

Total execution time: 115.0162 seconds

Press any key to exit

```

Modules (Double-click to edit a module)

Folder	Category	Description
Compound	Sync	Sync for new Macs, B...
Compound	Modules	Eric Zimmerman Parsers
EZTools	ProgramExecution	AmcacheParser; extr...
EZTools	ProgramExecution	AppCompatCachePar...
GitHub	Remote Access	BMC-Tools: RDP Bitn...
Compound	Modules	Run all strings Modu...
strings	KeywordSearches	Use strings to GREP...
strings	KeywordSearches	Use strings to GREP...

Key:

Value:

Target variables

Key:

Value:

Other options

Debug messages Trace messages Ignore FTK warning

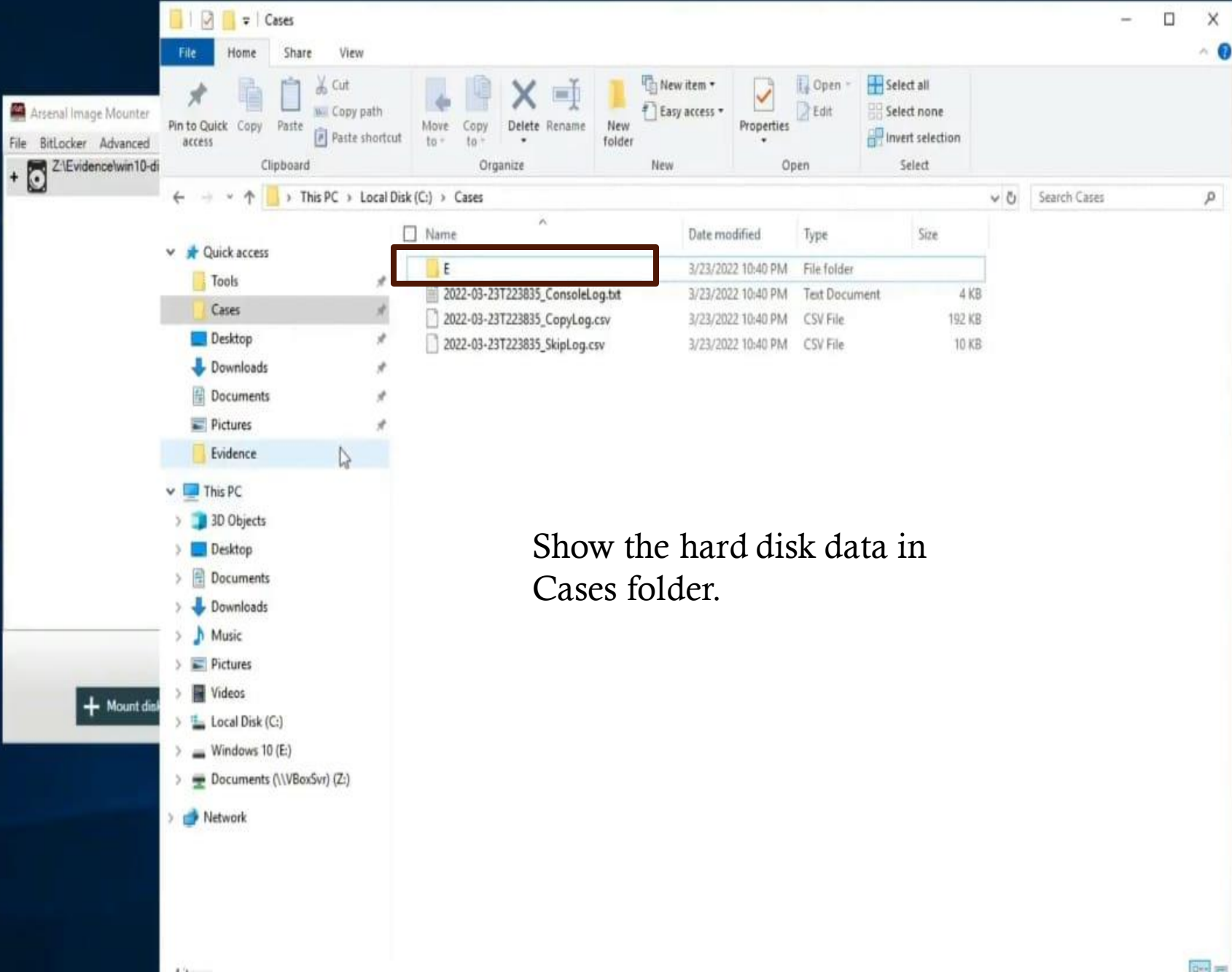
Zip password

Retain local copies

Current command line

```
.\kape.exe --tsource E: --tdest C:\Cases --tflush --target KapeTriage --ifw --gui
```


Documentation Targets available: 254 Targets selected: 1 Modules available: 253 Modules selected: 0 Disable flush warnings



Show the hard disk data in Cases folder.



Recycle Bin



Firefox



Notepad++



Event Log Explorer

Arsenal Image Mounter

File BitLocker Advanced

Z:\Evidence\win10-ds

+ Mount disk

Windows 10 (E)

File Home Share View Drive Tools

Clipboard: Pin to Quick access, Copy, Paste, Copy path, Paste shortcut

Organize: Move to, Copy to, Delete, Rename

New: New Item, Easy access, New folder

Open: Open, Properties, Edit

Select: Select all, Select none, Invert selection

This PC > Windows 10 (E)

Name	Date modified	Type	Size
AtomicRedTeam	3/18/2022 12:24 AM	File folder	
BGInfo	3/19/2019 11:30 AM	File folder	
PerfLogs	9/15/2018 7:33 AM	File folder	
Program Files	3/18/2022 12:22 AM	File folder	
Program Files (x86)	3/19/2019 11:33 AM	File folder	
ProgramData	3/18/2022 12:18 AM	File folder	
Users	3/19/2019 10:51 AM	File folder	
Windows	3/18/2022 12:18 AM	File folder	

0 items



Disk Analysis Process

Go to the link and Download the materials.

<https://github.com/bluecapesecurity/PWF/blob/main/Resources/Analysis-Notes-Template.docx>

Windows Registry

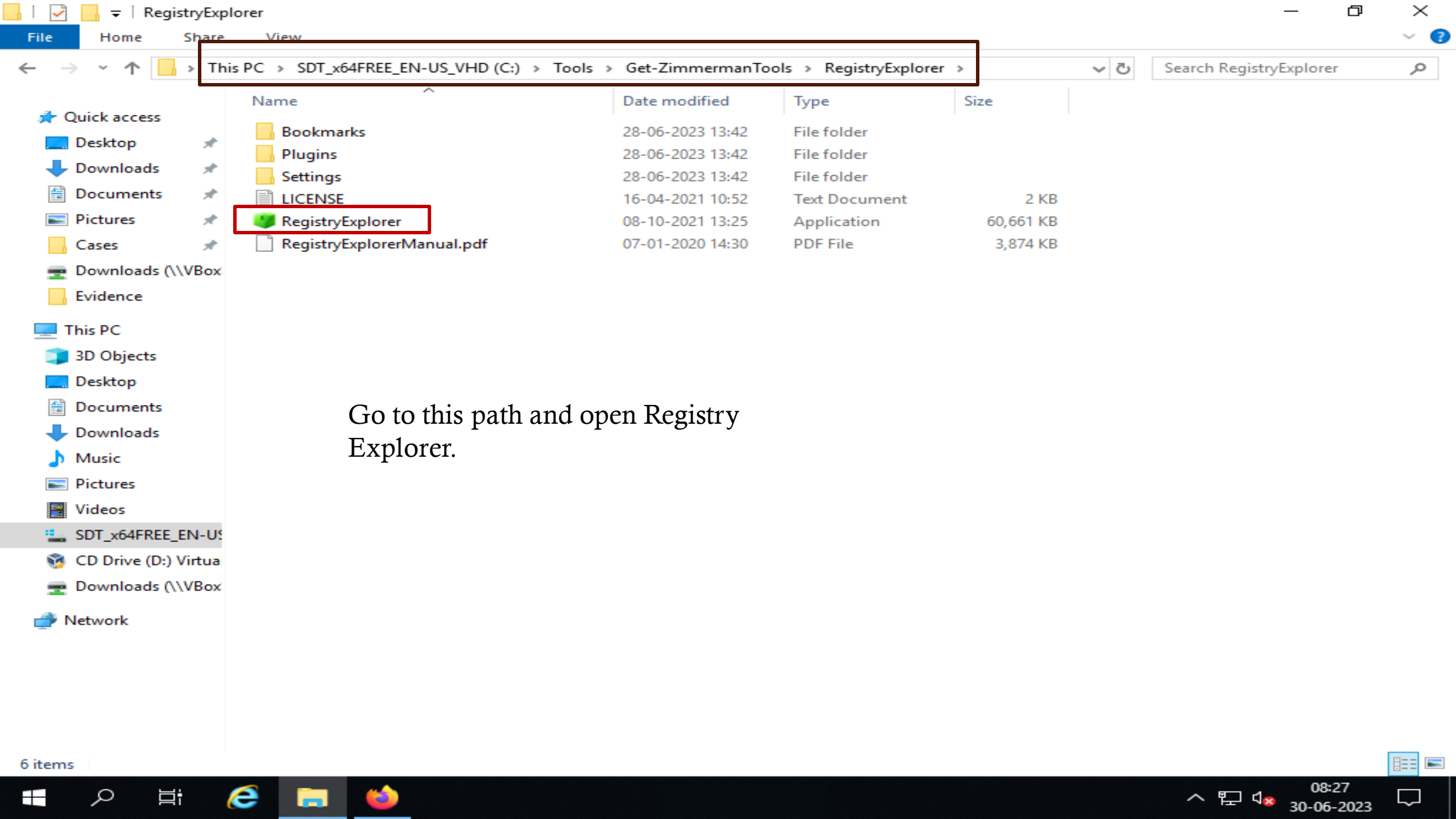
The **registry** or **Windows registry** is a database of information, settings, options, and other values for software and hardware installed on all versions of Microsoft Windows operating systems. When a program is installed, a new subkey is created in the registry. This subkey contains settings specific to that program, such as its location, version, and primary executable.

Registry Explorer with Eric Zimmerman Tools

The screenshot shows a Windows File Explorer window titled 'Get-ZimmermanTools'. The address bar indicates the path: 'This PC > SDT_x64FREE_EN-US_VHD (C:) > Tools > Get-ZimmermanTools'. The left sidebar shows 'Quick access' and 'This PC' sections. The main pane displays a list of 32 items with columns for Name, Date modified, Type, and Size. The 'RegistryExplorer' folder is highlighted with a red box.

Name	Date modified	Type	Size
EvtxECmd	28-06-2023 13:40	File folder	
EZViewer	28-06-2023 13:40	File folder	
Hasher	28-06-2023 13:41	File folder	
iisGeolocate	28-06-2023 13:44	File folder	
JumpListExplorer	28-06-2023 13:41	File folder	
MFTExplorer	28-06-2023 13:41	File folder	
RECmd	28-06-2023 13:41	File folder	
RegistryExplorer	28-06-2023 13:42	File folder	
SDBExplorer	28-06-2023 13:42	File folder	
ShellBagsExplorer	28-06-2023 13:43	File folder	
SQLCmd	28-06-2023 13:43	File folder	
TimelineExplorer	28-06-2023 13:43	File folder	
XWFIM	28-06-2023 13:44	File folder	
!!!RemoteFileDetails	28-06-2023 13:44	CSV File	5 KB
AmcacheParser	21-05-2023 11:49	Application	4,661 KB
AppCompatCacheParser	07-03-2023 15:13	Application	4,523 KB
bstrings	20-05-2022 12:38	Application	3,997 KB
ChangeLog	28-06-2023 13:44	Text Document	33 KB
Get-ZimmermanTools	18-05-2023 14:24	Windows PowerS...	24 KB
JLECmd	13-03-2023 17:06	Application	4,792 KB
LECmd	04-03-2023 10:30	Application	5,063 KB
MFTCmd	20-10-2022 13:37	Application	4,409 KB
PECmd	28-01-2022 12:08	Application	3,885 KB
RBCmd	05-08-2022 13:05	Application	3,607 KB
RecentFileCacheParser	15-06-2022 11:03	Application	3,283 KB
rla	28-11-2022 13:16	Application	4,261 KB
SBECmd	23-02-2022 08:38	Application	4,800 KB
SrumECmd	26-10-2022 09:41	Application	4,517 KB

32 items



This PC > SDT_x64FREE_EN-US_VHD (C:) > Tools > Get-ZimmermanTools > RegistryExplorer

Name	Date modified	Type	Size
Bookmarks	28-06-2023 13:42	File folder	
Plugins	28-06-2023 13:42	File folder	
Settings	28-06-2023 13:42	File folder	
LICENSE	16-04-2021 10:52	Text Document	2 KB
RegistryExplorer	08-10-2021 13:25	Application	60,661 KB
RegistryExplorerManual.pdf	07-01-2020 14:30	PDF File	3,874 KB

Go to this path and open Registry Explorer.

6 items



config

File Home Share View

Cases > F > Windows > System32 > config

Name	Date modified	Type	Size
DEFAULT	29-06-2023 09:08	File	512 KB
SAM	29-06-2023 09:08	File	64 KB
SECURITY	29-06-2023 09:08	File	32 KB
SOFTWARE	29-06-2023 09:08	File	68,608 KB
SYSTEM	29-06-2023 09:08	File	11,008 KB

5 items | 5 items selected 78.3 MB

Go to this path and load all Registry hives on Registry Explorer.



Recycle Bin



Firefox



Event Log Explorer



Notepad++

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (4/0) View Help

Registry hives (5) Available bookmarks (73/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
<ul style="list-style-type: none"> <ul style="list-style-type: none"> ROOT 	=	=	=
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> ROOT 	0	3	2023-06-29 08:01:15
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> Associated deleted records 	0	0	
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> Unassociated deleted values 	2	0	
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> ROOT 	0	1	2023-06-28 16:04:43
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> Associated deleted records 	0	0	
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> ROOT 	0	17	2023-06-29 08:00:59
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> Associated deleted records 	0	0	
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> Unassociated deleted records 	0	0	
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> Unassociated deleted values 	146	0	
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> ROOT 	0	17	2023-06-29 08:14:27
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> Associated deleted records 	0	0	
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> Unassociated deleted records 	0	0	
<ul style="list-style-type: none"> <ul style="list-style-type: none"> <ul style="list-style-type: none"> Unassociated deleted values 	46	0	

Values

Drag a column header here to group by that column

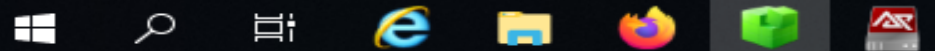
	Va...	V...	Data	Value Slack	Is Deleted
☿	=	=	=	=	=

Key: ROOT

Selected hive: SECURITY Last write: 2023-06-29 08:01:15 Key contains no values Load complete

Value: None

Build 17763.rs5_release.180914-1434



Enter text to search... Find

Key name
<ul style="list-style-type: none"> <ul style="list-style-type: none"> C:\Cases\F\Windows\System32\config\SECURITY C:\Cases\F\Windows\System32\config\DEFAULT C:\Cases\F\Windows\System32\config\SAM C:\Cases\F\Windows\System32\config\SYSTEM C:\Cases\F\Windows\System32\config\SOFTWARE <ul style="list-style-type: none"> Channels command Control Panel CurrentVersion CurrentVersion Windows Defender Windows Defender Devices

Using Software hives gathering the information about current version of OS.

Bookmark information

Hive: C:\Cases\F\Windows\System32\config\SOFTWARE

Category: Operating system

Name: CurrentVersion

Key path: Microsoft\Windows\CurrentVersion

Short description: Windows version information (Windows key)

Long description:

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value...	Is Del...	Data Rec...
ProgramFilesDir	RegSz	C:\Pr...	00-00	<input type="checkbox"/>	<input type="checkbox"/>
CommonFilesDir	RegSz	C:\Pr...		<input type="checkbox"/>	<input type="checkbox"/>
ProgramFilesDir (x86)	RegSz	C:\Pr...	00-00...	<input type="checkbox"/>	<input type="checkbox"/>
CommonFilesDir (x86)	RegSz	C:\Pr...	00-00...	<input type="checkbox"/>	<input type="checkbox"/>
CommonW6432Dir	RegSz	C:\Pr...		<input type="checkbox"/>	<input type="checkbox"/>
DevicePath	RegExpan...	%Sys...	00-00	<input type="checkbox"/>	<input type="checkbox"/>
MediaPathUnexpanded	RegExpan...	%Sys...	00-00...	<input type="checkbox"/>	<input type="checkbox"/>
ProgramFilesPath	RegExpan...	%Pro...	00-00...	<input type="checkbox"/>	<input type="checkbox"/>
ProgramW6432Dir	RegSz	C:\Pr...	00-00	<input type="checkbox"/>	<input type="checkbox"/>
SM_ConfigureProgramsN...	RegSz	Set P...	00-00...	<input type="checkbox"/>	<input type="checkbox"/>
SM_GamesName	RegSz	Games		<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Slack viewer Binary viewer

Value name: ProgramFilesDir

Value type: RegSz

Value: C:\Program Files

Raw value: 43-00-3A-00-5C-00-50-00-72-00-6F-00-67-00-72-00-61-00-6D-00-20-00-46-00-69-00-6C-00-65-00-73-00-00-00

Enter text to search... Find

Key name

- C:\Cases\F\Windows\System32\config\SECURITY
- C:\Cases\F\Windows\System32\config\DEFAULT
- C:\Cases\F\Windows\System32\config\SAM
- C:\Cases\F\Windows\System32\config\SYSTEM
 - {4d36e972-e325-11ce-bfc1-08002be10318}
 - {53f56307-b6bf-11d0-94f2-00a0c91efb8b}
 - {6bdd1fc6-810f-11d0-bec7-08002be2092f}
 - AppCompatCache
 - bam
 - Devices
 - ComputerName**
 - CrashControl
 - DeviceClasses

Using System hive gathering the information about computer name of target system.

Bookmark information

Hive: C:\Cases\F\Windows\System32\config\SYSTEM

Category: Operating system

Name: ComputerName

Key path: ControlSet001\Control\ComputerName\ComputerName

Short description: The name of the computer

Long description: The name of the computer

Key: ControlSet001\Control\ComputerName\ComputerName

Selected hive: SECURITY Last write: 28-06-2023 16:12:11 +00:00 2 of 2 values shown (100.00%) Copied Value data to clipboard Hidden keys: 0 1

Values

Drag a column header here to group by that column

	Value Name	Value Type	Data	Value ...	Is Del...	Data Re...
	(default)	RegSz	mnmsrvc	02-00...	<input type="checkbox"/>	<input type="checkbox"/>
	ComputerName	RegSz	DESKTOP-MD2HC...	01-00...	<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Slack viewer Binary viewer

Value name: ComputerName

Value type: RegSz

Value: DESKTOP-MD2HCPT

Raw value: 44-00-45-00-53-00-4B-00-54-00-4F-00-50-00-2D-00-4D-00-44-00-32-00-48-00-43-00-50-00-54-00-00-00

Gathering system information with RegRipper

Follow the Step for Regripper

1. Go to the `C:\Tools\RegRipper\ > open cmd > dir > rip.exe`
2. You can create a folder in c drive with Analysis and also create registry folder in Analysis
3. Insert the file in Analysis folder:

```
C:\Cases\F\Windows\system32\config - DEFAULT  
                                     SAM  
                                     SECURITY  
                                     SOFTWARE  
                                     SYSTEM
```

```
C:\Cases\F\users\Denisha - NTUSER.DAT
```

```
C:\Cases\F\users\Denisha\AppData\Local\Microsoft\Windows\ - UserClass.dat
```

4. Back to cmd and type `rip.exe -r C:\Cases\Analysis\Registry\SOFTWARE -p winver`
5. `rip.exe -r C:\Cases\Analysis\Registry\SOFTWARE -p nic2`
6. `rip.exe -r C:\Cases\Analysis\Registry\SYSTEM -p timezone`
7. `rip.exe -r C:\Cases\Analysis\Registry\SYSTEM -p shutdown`
8. `rip.exe -r C:\Cases\Analysis\Registry\SOFTWARE -p defender`

File Explorer window showing the directory `C:\Tools\RegRipper3.0-master\RegRipper3.0-master`. The address bar is highlighted with a red box.

Name	Date modified	Type	Size
plugins	01-07-2023 06:42	File folder	
.gitattributes	21-03-2023 11:46	GITATTRIBUTES File	1 KB
Base.pm	21-03-2023 11:46	PM File	27 KB
File.pm	21-03-2023 11:46	PM File	9 KB
Key.pm	21-03-2023 11:46	PM File	14 KB
license.md	21-03-2023 11:46	MD File	2 KB
license	21-03-2023 11:46	Text Document	2 KB
p2x5124.dll	21-03-2023 11:46	Application extens...	417 KB
q	21-03-2023 11:46	Icon	6 KB
README.md	21-03-2023 11:46	MD File	2 KB
regrip	21-03-2023 11:46	Windows Batch File	1 KB
rip	21-03-2023 11:46	Application	1,857 KB
rip	21-03-2023 11:46	PL File	17 KB
rip_bulk	21-03-2023 11:46	Compressed (zipp...	1,591 KB
rr	21-03-2023 11:46	Application	2,492 KB
rr	21-03-2023 11:46	PL File	16 KB

Go to this path and open cmd.

Administrator: C:\Windows\System32\cmd.exe

Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Tools\RegRipper3.0-master\RegRipper3.0-master>rip.exe

Rip v.3.0 - CLI RegRipper tool
Rip [-r Reg hive file] [-f profile] [-p plugin] [options]
Parse Windows Registry files, using either a single module, or a profile.

NOTE: This tool does NOT automatically process Registry transaction logs! The tool does check to see if the hive is dirty, but does not automatically process the transaction logs. If you need to incorporate transaction logs, please consider using yarp + registryFlush.py, or rla.exe from Eric Zimmerman.

-r [hive]Registry hive file to parse
-dCheck to see if the hive is dirty
-gGuess the hive file type
-aAutomatically run hive-specific plugins
-aTAutomatically run hive-specific TLN plugins
-f [profile].....use the profile
-p [plugin].....use the plugin
-llist all plugins
-cOutput plugin list in CSV format (use with -l)
-s systemname.....system name (TLN support)
-u username.....User name (TLN support)
-uPUpdate default profiles
-h.....Help (print this information)

Ex: C:\>rip -r c:\case\system -f system
C:\>rip -r c:\case\ntuser.dat -p userassist
C:\>rip -r c:\case\ntuser.dat -a

Downloads (\\V)

16 items



09:16

09-07-2023



```
-s systemname.....system name (TLN support)
-u username.....User name (TLN support)
-uP .....Update default profiles
-h.....Help (print this information)
```

```
Ex: C:\>rip -r c:\case\system -f system
    C:\>rip -r c:\case\ntuser.dat -p userassist
    C:\>rip -r c:\case\ntuser.dat -a
    C:\>rip -l -c
```

All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.

copyright 2020 Quantum Analytics Research, LLC

```
C:\Tools\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r C:\Cases\Analysis\Registry\SOFTWARE -p winver
```

```
Launching winver v.20200525
```

```
winver v.20200525
```

```
(Software) Get Windows version & build info
```

```
ProductName           Windows 10 Enterprise Evaluation
ReleaseID              2009
BuildLab               19041.vb_release.191206-1406
BuildLabEx             19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID  EnterpriseEval
RegisteredOrganization
RegisteredOwner        Denisha
InstallDate            2023-06-28 16:13:27Z
InstallTime            2023-06-28 16:13:27Z
```

```
C:\Tools\RegRipper3.0-master\RegRipper3.0-master>
```

Using plugins gathering more details
Here using winver plugin show detail
about windows version.



Microsoft Windows [Version 10.0.17763.737]

(c) 2018 Microsoft Corporation. All rights reserved.

C:\Tools\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r C:\Cases\Analysis\Registry\SYSTEM -p timezone

Launching timezone v.20200518

timezone v.20200518

(System) Get TimeZoneInformation key contents

TimeZoneInformation key

ControlSet001\Control\TimeZoneInformation

LastWrite Time 2023-06-28 16:04:24Z

DaylightName -> @tzres.dll,-491

StandardName -> @tzres.dll,-492

Bias -> -330 (-5.5 hours)

ActiveTimeBias -> -330 (-5.5 hours)

TimeZoneKeyName-> India Standard Time

Timezone plugin use for
detail about time.

C:\Tools\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r C:\Cases\Analysis\Registry\SYSTEM -p nic2

Launching nic2 v.20200525

nic2 v.20200525

(System) Gets NIC info from System hive

Adapter: {546a6a36-9c1a-46da-b144-6768b13c717c}

LastWrite Time: 2023-06-28 16:04:51Z

EnableDHCP 1

Domain

NameServer

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.

Adapter: {737b8094-15cd-11ee-a176-806e6f6e6963}

LastWrite Time: 2023-06-28 16:05:14Z

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.

Adapter: {f2d726a5-0133-4845-bbf7-20d9e13d48bd}

LastWrite Time: 2023-06-29 08:01:18Z

EnableDHCP 1

Domain

NameServer

DhcpIPAddress 10.0.2.15

DhcpSubnetMask 255.255.255.0

DhcpServer 10.0.2.2

Lease 86400

LeaseObtainedTime 2023-06-29 08:01:18Z

T1 2023-06-29 20:01:18Z

Nic2 plugin use for
detail about network
card.

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.

C:\Tools\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r C:\Cases\Analysis\Registry\SYSTEM -p networklist

Launching networklist v.20200518

Launching networklist v.20200518

(Software) Collects network info from NetworkList key

Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles not found.

C:\Tools\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r C:\Cases\Analysis\Registry\SYSTEM -p shutdown

Launching shutdown v.20200518

shutdown v.20200518

(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value

LastWrite time: 2023-06-29 09:08:05Z

ShutdownTime : 2023-06-29 09:08:05Z

Detail about last shutdown time of target system.

C:\Tools\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r C:\Cases\Analysis\Registry\SOFTWARE -P defender

Launching defender v.20200427

defender v.20200427

(Software) Get Windows Defender settings

Key path: Microsoft\Windows Defender

LastWrite Time 2023-06-29 09:07:52Z

Detail about Microsoft defender

Key path: Microsoft\Windows Defender\Exclusions\Paths

Key path: Microsoft\Windows Defender\Exclusions\Extensions

Key path: Microsoft\Windows Defender\Exclusions\Processes

Key path: Microsoft\Windows Defender\Exclusions\TemporaryPaths

Key path: Microsoft\Windows Defender\Exclusions\IpAddresses

Key path: Microsoft\Windows Defender\Features

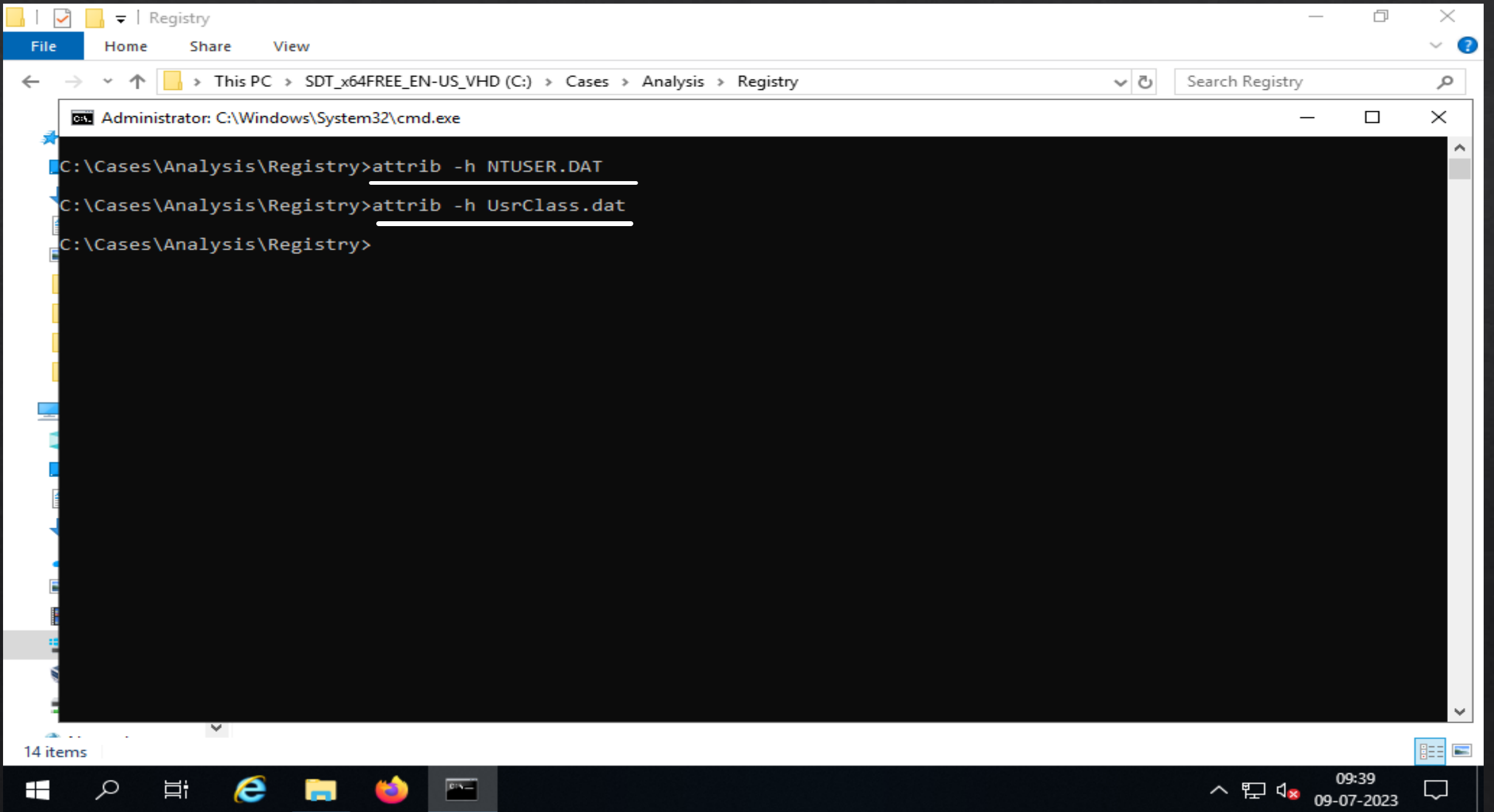
TamperProtection value = 1

If TamperProtection value = 1, it's disabled

Key path: Microsoft\Windows Defender\Real-Time Protection

Parsing registry hives in bulk with RegRipper

1. Go to the Registry folder location > open cmd > dir > attrib * > attrib -h NTUSER\DAT > attrib -h UserClass.dat
2. For /r %i in (*) do (C:\Tools\RegRipper\rip.exe -r %i -a > %i.txt).
3. Show in Registry folder text file automatic created then after all file selected and edit with Notepad++ and show the all detail of target system.



```
29-06-2023 09:08          524,288 DEFAULT
29-06-2023 09:08          65,536 SAM
29-06-2023 09:08          32,768 SECURITY
29-06-2023 09:08       70,254,592 SOFTWARE
29-06-2023 09:08       11,272,192 SYSTEM
          5 File(s)      82,149,376 bytes
          2 Dir(s)    22,986,297,344 bytes free
```

```
C:\Cases\Analysis\Registry>attrib *
```

```
A          C:\Cases\Analysis\Registry\DEFAULT
A H       C:\Cases\Analysis\Registry\NTUSER.DAT
A          C:\Cases\Analysis\Registry\SAM
A          C:\Cases\Analysis\Registry\SECURITY
A          C:\Cases\Analysis\Registry\SOFTWARE
A          C:\Cases\Analysis\Registry\SYSTEM
```

```
C:\Cases\Analysis\Registry>attrib -h NTUSER.DAT
```

```
C:\Cases\Analysis\Registry>for /r %i in (*) do (C:\Tools\RegRipper3.0-master\RegRipper3.0-master\rip.exe -r %i -a > %i.txt)
```

```
C:\Cases\Analysis\Registry>(C:\Tools\RegRipper3.0-master\RegRipper3.0-master\rip.exe -r C:\Cases\Analysis\Registry\DEFAULT -a
1>C:\Cases\Analysis\Registry\DEFAULT.txt )
```

```
Launching adobe v.20200522
Launching allowedenum v.20200511
Launching appassoc v.20200515
Launching appcompatflags v.20200525
Launching appkeys v.20200517
Launching applets v.20200525
Launching apppaths v.20200511
Launching appspecific v.20200515
Launching appx v.20200427
Launching arpcache v.20200515
Launching attachmgr v.20200525
Launching cached v.20200525
Launching cmdproc v.20200515
Launching comdlg32 v.20200517
Launching compdesc v.20200511
Launching DDO v.20140414
Launching disablemru v.20190924
Launching environment v.20200512
Launching featureusage v.20200511
[*] Launching heidisql v.20201227
[*] Launching iconlayouts v.20211001
Launching identities v.20200525
```

Execute the command for create the text file of registry hives.

Registry

File Home Share View

This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > Analysis > Registry

Search Registry

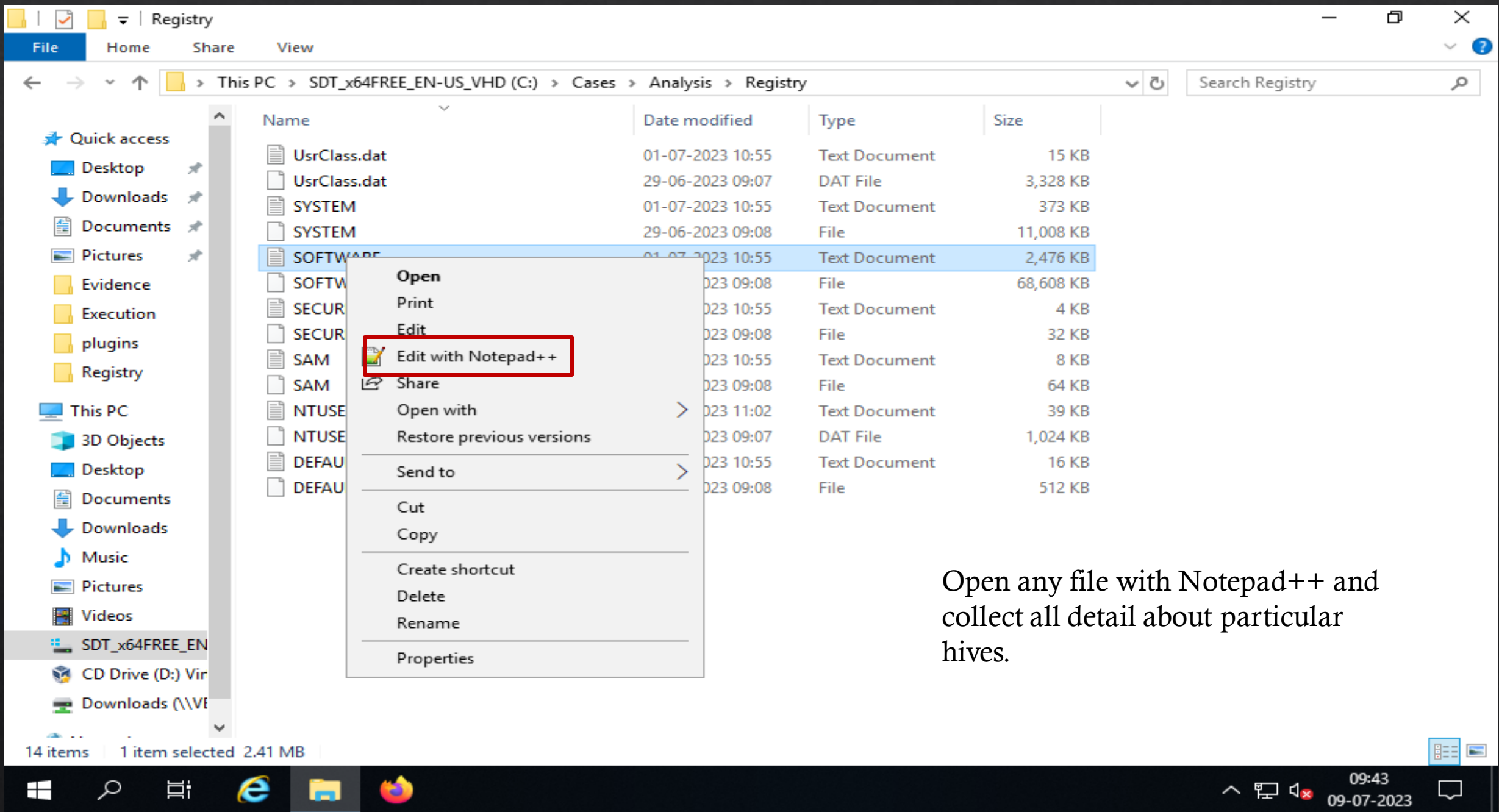
Name	Date modified	Type	Size
UsrClass.dat	01-07-2023 10:55	Text Document	15 KB
UsrClass.dat	29-06-2023 09:07	DAT File	3,328 KB
SYSTEM	01-07-2023 10:55	Text Document	373 KB
SYSTEM	29-06-2023 09:08	File	11,008 KB
SOFTWARE	01-07-2023 10:55	Text Document	2,476 KB
SOFTWARE	29-06-2023 09:08	File	68,608 KB
SECURITY	01-07-2023 10:55	Text Document	4 KB
SECURITY	29-06-2023 09:08	File	32 KB
SAM	01-07-2023 10:55	Text Document	8 KB
SAM	29-06-2023 09:08	File	64 KB
NTUSER.DAT	01-07-2023 11:02	Text Document	39 KB
NTUSER.DAT	29-06-2023 09:07	DAT File	1,024 KB
DEFAULT	01-07-2023 10:55	Text Document	16 KB
DEFAULT	29-06-2023 09:08	File	512 KB

14 items

Show the all text file of registry hives.

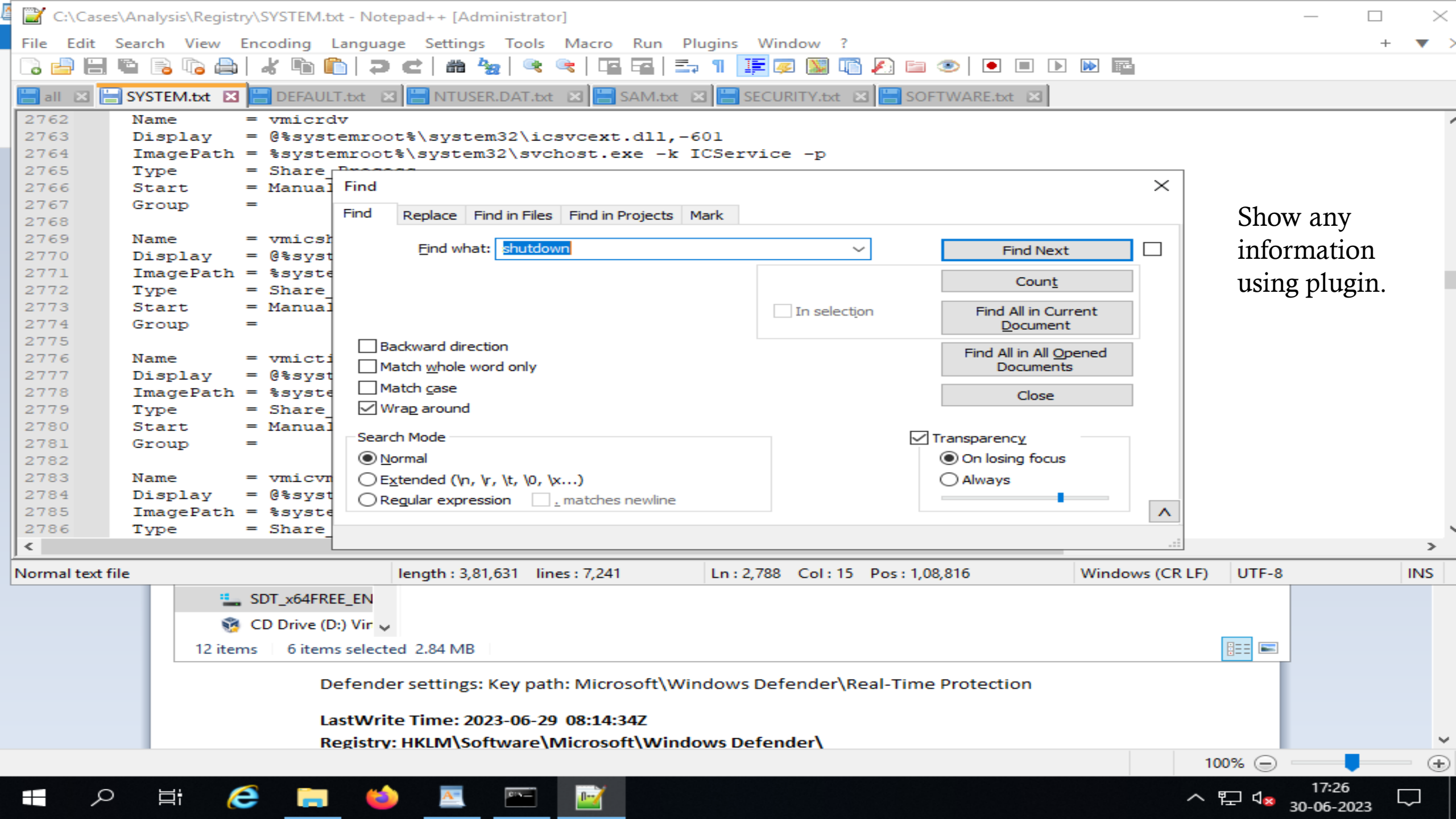


09:36
09-07-2023

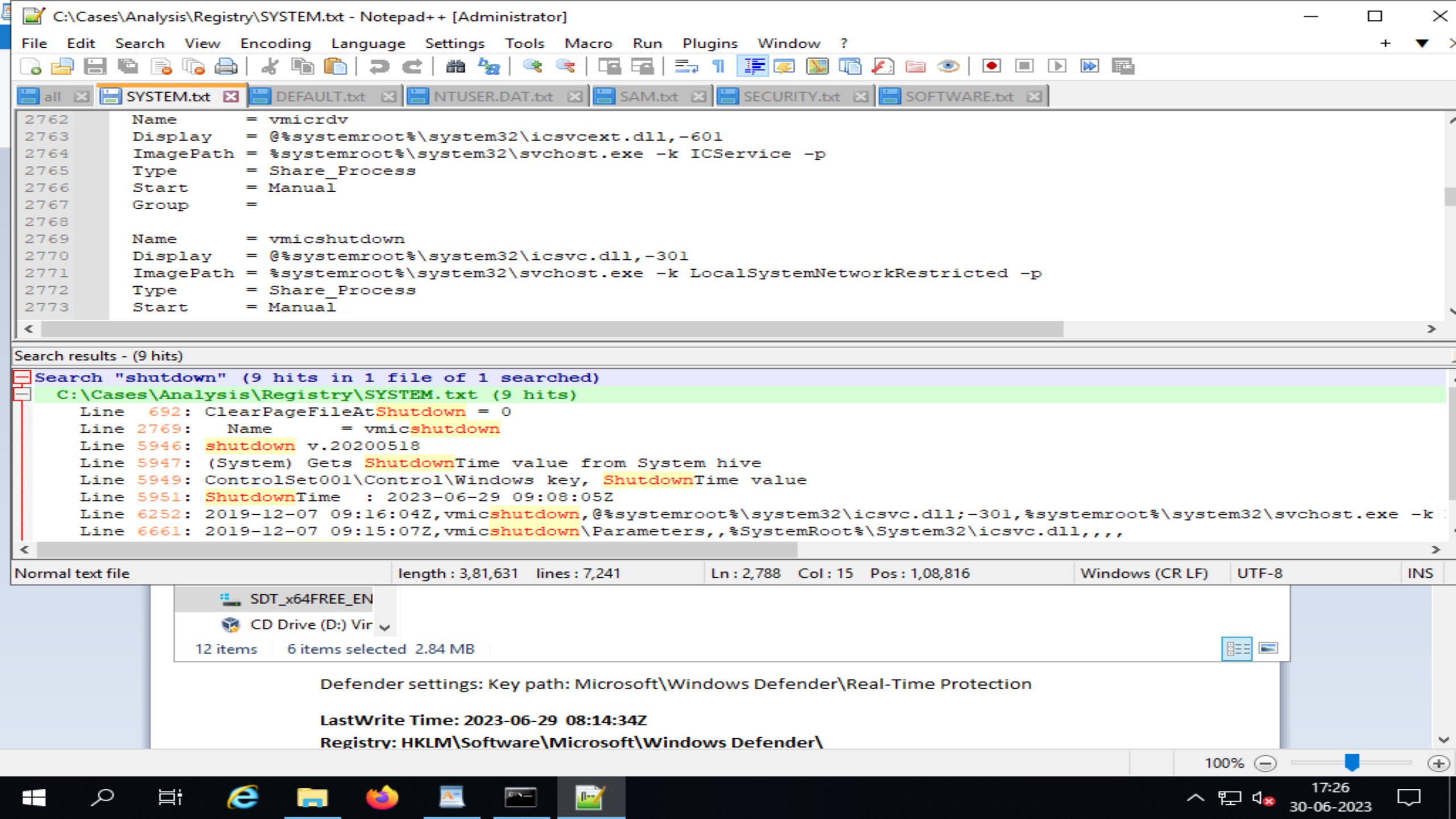


Name	Date modified	Type	Size
UsrClass.dat	01-07-2023 10:55	Text Document	15 KB
UsrClass.dat	29-06-2023 09:07	DAT File	3,328 KB
SYSTEM	01-07-2023 10:55	Text Document	373 KB
SYSTEM	29-06-2023 09:08	File	11,008 KB
SOFTWARE	01-07-2023 10:55	Text Document	2,476 KB
SOFTWARE	2023 09:08	File	68,608 KB
SECUR	2023 10:55	Text Document	4 KB
SECUR	2023 09:08	File	32 KB
SAM	2023 10:55	Text Document	8 KB
SAM	2023 09:08	File	64 KB
NTUSE	2023 11:02	Text Document	39 KB
NTUSE	2023 09:07	DAT File	1,024 KB
DEFAU	2023 10:55	Text Document	16 KB
DEFAU	2023 09:08	File	512 KB

Open any file with Notepad++ and collect all detail about particular hives.



Show any information using plugin.



```
2762 Name = vmicrdv
2763 Display = @%systemroot%\system32\icsvcext.dll,-601
2764 ImagePath = %systemroot%\system32\svchost.exe -k ICService -p
2765 Type = Share_Process
2766 Start = Manual
2767 Group =
2768
2769 Name = vmicshutdown
2770 Display = @%systemroot%\system32\icsvc.dll,-301
2771 ImagePath = %systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted -p
2772 Type = Share_Process
2773 Start = Manual
```

Search results - (9 hits)

Search "shutdown" (9 hits in 1 file of 1 searched)

C:\Cases\Analysis\Registry\SYSTEM.txt (9 hits)

```
Line 692: ClearPageFileAtShutdown = 0
Line 2769: Name = vmicshutdown
Line 5946: shutdown v.20200518
Line 5947: (System) Gets ShutdownTime value from System hive
Line 5949: ControlSet001\Control\Windows key, ShutdownTime value
Line 5951: ShutdownTime : 2023-06-29 09:08:05Z
Line 6252: 2019-12-07 09:16:04Z, vmicshutdown, @%systemroot%\system32\icsvc.dll;-301,%systemroot%\system32\svchost.exe -k
Line 6661: 2019-12-07 09:15:07Z, vmicshutdown\Parameters,, %SystemRoot%\System32\icsvc.dll,,,
```

SDT_x64FREE_EN
CD Drive (D:) Vir
12 items 6 items selected 2.84 MB

Defender settings: Key path: Microsoft\Windows Defender\Real-Time Protection
LastWrite Time: 2023-06-29 08:14:34Z
Registry: HKLM\Software\Microsoft\Windows Defender\

User Accounts and SIDs Overview

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net
The syntax of this command is:

NET
 [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\Administrator>net accounts
Force user logoff how long after time expires?:      Never
Minimum password age (days):                       0
Maximum password age (days):                       42
Minimum password length:                            0
Length of password history maintained:               None
Lockout threshold:                                  Never
Lockout duration (minutes):                          30
Lockout observation window (minutes):                30
Computer role:                                       SERVER
The command completed successfully.

C:\Users\Administrator>net user
User accounts for \\WIN-AJDB7G0IQEJ

-----
Administrator          DefaultAccount      Guest
WDAGUtilityAccount
The command completed successfully.

C:\Users\Administrator>net localgroup
Aliases for \\WIN-AJDB7G0IQEJ

-----
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Certificate Service DCOM Access
*Cryptographic Operators
```



```
C:\Users\Administrator>net localgroup
```

```
Aliases for \\WIN-AJDB7GOIQEJ
```

```
-----  
*Access Control Assistance Operators  
*Administrators  
*Backup Operators  
*Certificate Service DCOM Access  
*Cryptographic Operators  
*Device Owners  
*Distributed COM Users  
*Event Log Readers  
*Guests  
*Hyper-V Administrators  
*IIS_IUSRS  
*Network Configuration Operators  
*Performance Log Users  
*Performance Monitor Users  
*Power Users  
*Print Operators  
*RDS Endpoint Servers  
*RDS Management Servers  
*RDS Remote Access Servers  
*Remote Desktop Users  
*Remote Management Users  
*Replicator  
*Storage Replica Administrators  
*System Managed Accounts Group  
*Users
```

```
The command completed successfully.
```

```
C:\Users\Administrator>whoami  
win-ajdb7goiqej\administrator
```

```
C:\Users\Administrator>whoami /user
```

```
USER INFORMATION
```

```
-----
```

```
User Name
```

```
SID
```

```
-----
```



05:25
01-07-2023



*Users

The command completed successfully.

C:\Users\Administrator>whoami
win-ajdb7goiqej\administrator

C:\Users\Administrator>whoami /user

USER INFORMATION

User Name	SID
win-ajdb7goiqej\administrator	S-1-5-21-3369172402-319990300-3115234934-500

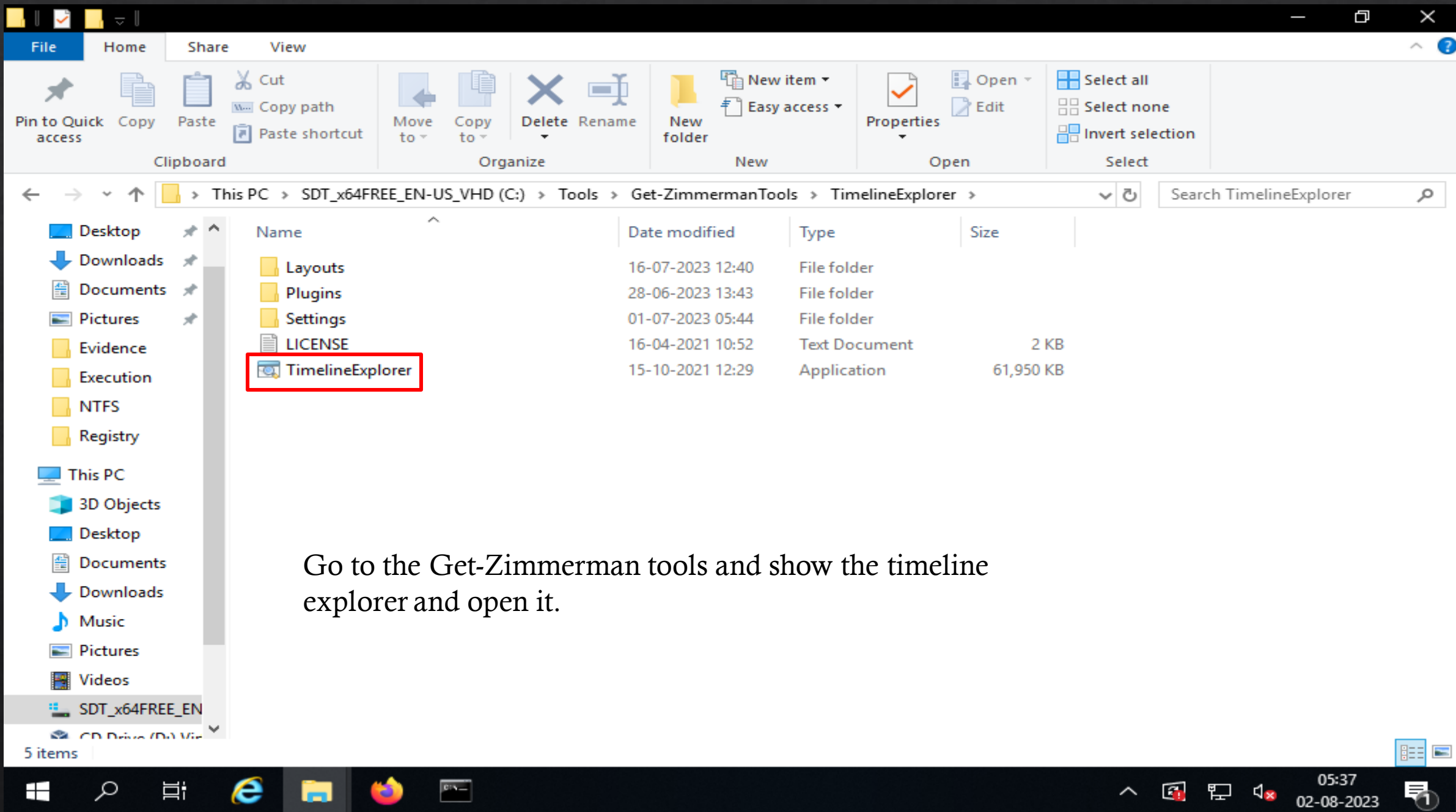
C:\Users\Administrator>_

File Explorer window showing the Desktop folder. The address bar indicates the path: This PC > Desktop. The left sidebar shows the navigation pane with 'Desktop' selected under 'This PC'. The main pane displays a list of files:

Name	Date modified	Type	Size
book	05-07-2023 05:18	Office Open XML ...	8 KB
Event Log Explorer	28-06-2023 13:23	Shortcut	2 KB
User accounts_Values_Export_2023070105...	01-07-2023 05:48	XLSX File	7 KB

An arrow points to the 'Event Log Explorer' file. Below the arrow, the text reads: "Open this file in timeline explorer".

Open this file in
timeline explorer



Go to the Get-Zimmerman tools and show the timeline explorer and open it.



Recycle Bin



Firefox



Event Log Explorer



Notepad++



book



User accounts_V...

Timeline Explorer v1.3.0.0

File Tools Tabs View Help



Please Wait

Loading file 'User accounts_Values_Export_20230701054831.xlsx'...



05:49

01-07-2023



1

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

User accounts_Values_Export_20230701054831.xlsx

Drag a column header here to group by that column

Enter text to search... Find

Created On	Last Login Time	Last Password Change	Last Incorrect Password	Expires On	User Name
=	=	=	RB C	RB C	RB C
2023-06-28 ...					Administrator
2023-06-28 ...					Guest
2023-06-28 ...					DefaultAccount
2023-06-28 ...		2023-06-28 16:04:43			WDAGUtilityAccount
2023-06-28 ...	2023-06-29 08:01...				Denisha
2023-06-28 ...	2023-06-28 16:18...	2023-06-28 16:12:17			defaultuser0

Show the detail about
Target system user.

Registry

File Home Share View

← → ↑ This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > Analysis > Registry Search Registry

Name	Date modified	Type	Size
DEFAULT	29-06-2023 09:08	File	512 KB
DEFAULT	30-06-2023 17:18	Text Document	16 KB
NTUSER.DAT	29-06-2023 09:07	DAT File	1,024 KB
NTUSER.DAT	30-06-2023 17:18	Text Document	39 KB
SAM	29-06-2023 09:08	File	64 KB
SAM	6-2023 17:18	Text Document	8 KB
SEC	6-2023 09:08	File	32 KB
SEC	6-2023 17:18	Text Document	4 KB
SO	6-2023 09:08	File	68,608 KB
SO	6-2023 17:19	Text Document	2,476 KB
SYS	6-2023 09:08	File	11,008 KB
SYS	6-2023 17:19	Text Document	373 KB

Open
Print
Edit
Edit with Notepad++
Share
Open with >
Restore previous versions
Send to >
Cut
Copy
Create shortcut
Delete
Rename
Properties

SAM file open with notepad++

12 items | 1 item selected 7.09 KB

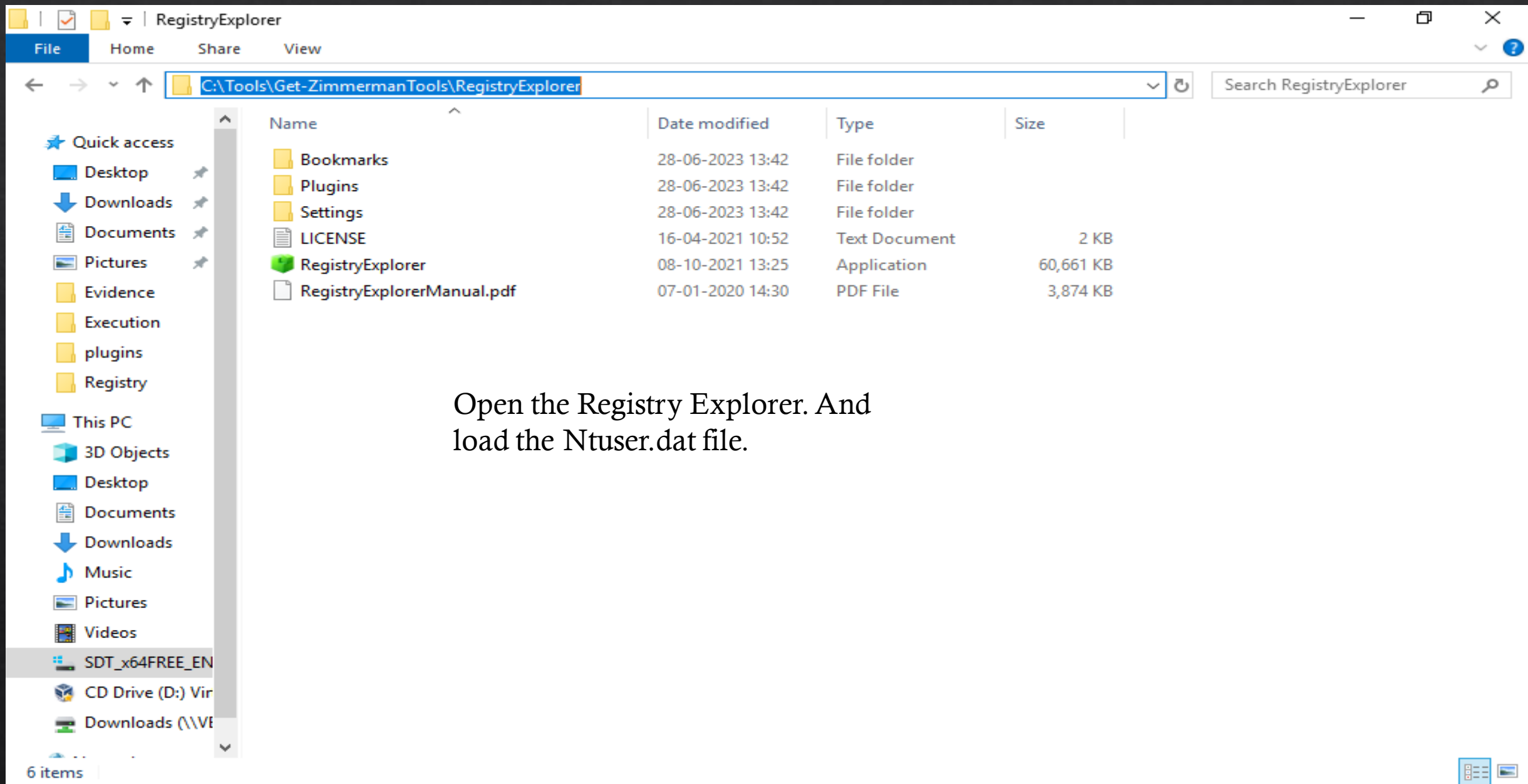

```
C:\Cases\Analysis\Registry\SAM.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
all SYSTEM.txt DEFAULT.txt NTUSER.DAT.txt SAM.txt SECURITY.txt SOFTWARE.txt
1 samparse v.20220921
2 (SAM) Parse SAM file for user & group mbrshp info
3
4
5 User Information
6 -----
7 Username      : Administrator [500]
8 SID           : S-1-5-21-3331464962-214784631-3394824829-500
9 Full Name     :
10 User Comment  : Built-in account for administering the computer/domain
11 Account Type  :
12 Account Created : Wed Jun 28 16:13:16 2023 Z
13 Name         :
14 Last Login Date : Never
15 Pwd Reset Date : Never
16 Pwd Fail Date  : Never
17 Login Count   : 0
18 --> Password does not expire
19 --> Account Disabled
20 --> Normal user account
21
22 Username      : Guest [501]
23 SID           : S-1-5-21-3331464962-214784631-3394824829-501
24 Full Name     :
25 User Comment  : Built-in account for guest access to the computer/domain
26 Account Type  :
27 Account Created : Wed Jun 28 16:13:16 2023 Z
28 Name         :
29 Last Login Date : Never
30 Pwd Reset Date : Never
31 Pwd Fail Date  : Never
32
```

Show the user detail using Notepad++.

RecentDocs Analysis

Information about the files that were recently opened/saved and the folders that were opened are maintained in the RecentDocs registry key.

Load the Ntuser.dat hive on Registry Explorer. And open Recent Doc.



Open the Registry Explorer. And load the Ntuser.dat file.



Registry Explorer v1.6.0.0

File Tools Options Bookmarks (29/0) View Help

Registry hives (1) Available bookmarks (29/0)

Enter text to search...

Find

Key name	# values
HKEY_CURRENT_USER	=
PrinterPorts	
RecentDocs	
.pdf	
.ps1	
.psd1	
.psm1	
.zip	
Folder	

Bookmark information

Hive

C:\Cases\Analysis\Registry\NTUSER.DAT

Category

User files and folders

Name

RecentDocs

Key path

Software\Microsoft\Windows\CurrentVersion\Explorer

Short description

Recently opened files by extension

Long description

See MRU key for order of opening

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Value: MRUListEx Collapse all hives

Selected hive: NTUSER.DAT Last write: 28-06-2023 17:58:22 +00:00 11 of 11 values shown (100.00%)

Hidden keys: 0 1

Values Recent documents

Drag a column header here to group by that column

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Las...
RecentDocs	8	invoke-atomicredteam	invoke-atomicredteam (2).lnk	=	=	=
RecentDocs	9	Invoke-AtomicRedTeam.psm1	Invoke-AtomicRedTeam (3).lnk	1		2023-06-28 1...
RecentDocs	7	Invoke-AtomicRedTeam.psd1	Invoke-AtomicRedTeam.lnk	2		2023-06-28 1...
RecentDocs	3	AtomicRedTeam	AtomicRedTeam.lnk	3		
RecentDocs	2	ART-attack.ps1	ART-attack.lnk	4		2023-06-28 1...
RecentDocs	6	Resources	Resources.lnk	5		
RecentDocs	5	PracticalWindowsForensics-cheat-sheet.pdf	PracticalWindowsForensics-cheat-sheet.lnk	6		2023-06-28 1...
RecentDocs	4	PWF-main.zip	PWF-main.lnk	7		2023-06-28 1...
RecentDocs	1	The Internet	The Internet.lnk	8		

Total rows: 19

Export ?

Type viewer

00000000	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E
08 00 00 00 09 00 00 00 07 00 00 00 03 00 00

Current offset: 0 (0x0) Bytes selected: 0 (0x0) Data interpreter: ?

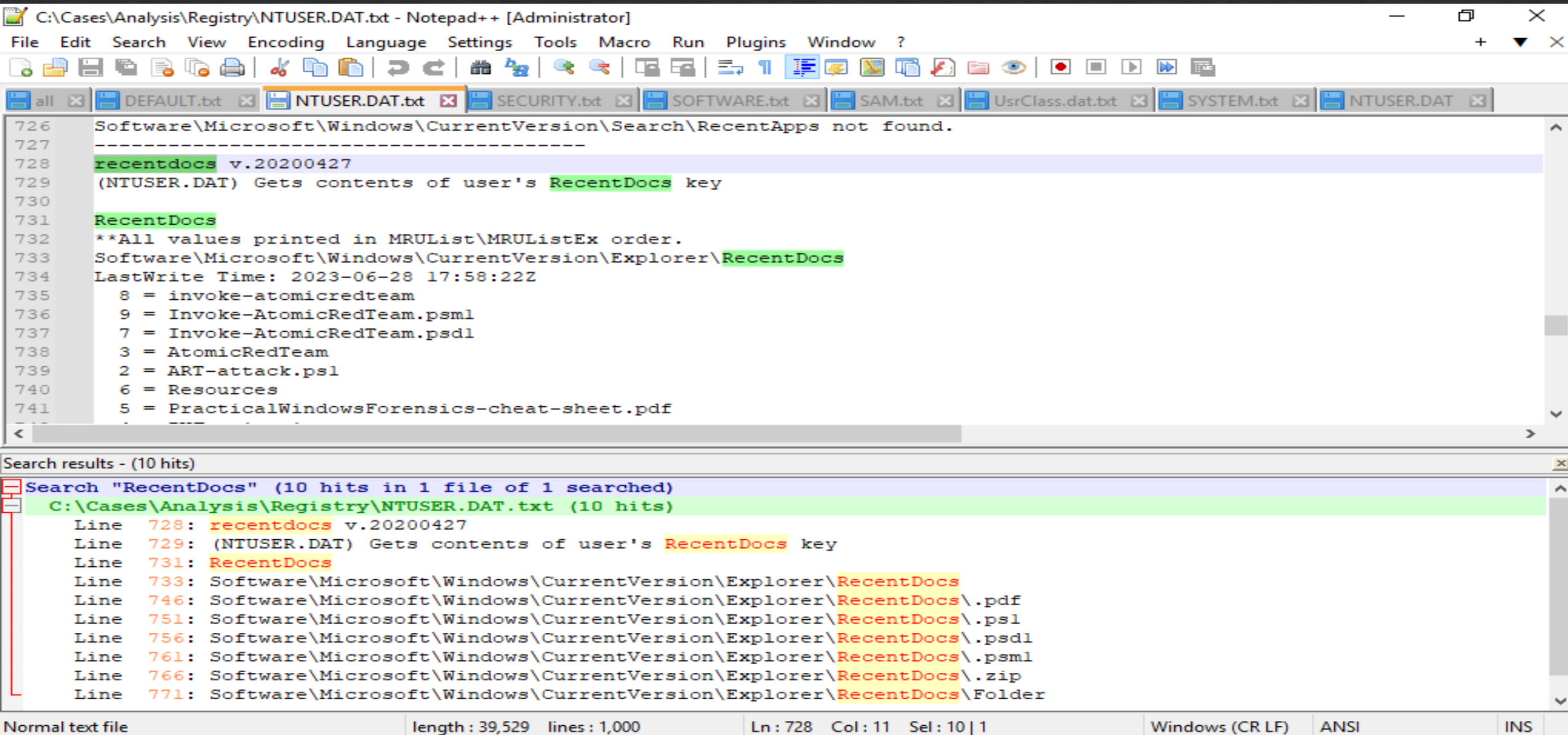


10:19

09-07-2023



Open Ntuser.dat file in Notepad++.



The image shows a Notepad++ window with the file `C:\Cases\Analysis\Registry\NTUSER.DAT.txt` open. The main text area contains the following content:

```
726 Software\Microsoft\Windows\CurrentVersion\Search\RecentApps not found.
727 -----
728 recentdocs v.20200427
729 (NTUSER.DAT) Gets contents of user's RecentDocs key
730
731 RecentDocs
732 **All values printed in MRUList\MRUListEx order.
733 Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
734 LastWrite Time: 2023-06-28 17:58:22Z
735     8 = invoke-atomicredteam
736     9 = Invoke-AtomicRedTeam.psml
737     7 = Invoke-AtomicRedTeam.psdl
738     3 = AtomicRedTeam
739     2 = ART-attack.psl
740     6 = Resources
741     5 = PracticalWindowsForensics-cheat-sheet.pdf
```

Below the main text area, a search results pane is visible, showing 10 hits for the search term "RecentDocs". The results are as follows:

```
Search results - (10 hits)
Search "RecentDocs" (10 hits in 1 file of 1 searched)
C:\Cases\Analysis\Registry\NTUSER.DAT.txt (10 hits)
Line 728: recentdocs v.20200427
Line 729: (NTUSER.DAT) Gets contents of user's RecentDocs key
Line 731: RecentDocs
Line 733: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
Line 746: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf
Line 751: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psl
Line 756: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psdl
Line 761: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.psml
Line 766: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.zip
Line 771: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
```

The status bar at the bottom of the Notepad++ window displays the following information: "Normal text file", "length: 39,529", "lines: 1,000", "Ln: 728", "Col: 11", "Sel: 10 | 1", "Windows (CR LF)", "ANSI", and "INS".

ShellBags Analysis

Analysis of shellbags is useful as it can aid in the creating a broader picture of an investigation, providing indications of activity, acting as a history of what directory items may have since been removed from a system, or even evidence access of removable devices where are no longer attached. And also store Malicious Activity.

Usrclass.txt file edit with Notepad++.

```
C:\Cases\Analysis\Registry\UsrClass.dat.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
all x DEFAULT.txt x NTUSER.DAT.txt x SECURITY.txt x SOFTWARE.txt x SAM.txt x UsrClass.dat.txt x SYSTEM.txt x
127 -----
128 | | | | | | | My Games [Desktop\0\]
129 | | | | | | | My Computer [Desktop\1\]
130 | | | | | | | My Computer\D:\ [Desktop\1\0\]
131 | | | | | | | My Computer\Z:\ [Desktop\1\1\]
132 | | | | | | | My Computer\CLSID_Desktop [Desktop\1\]
133 | 2023-06-28 16:33:34 | 2023-06-28 16:33:32 | | | 99809/3 | My Computer\CLSID_Desktop\PWF-main [Desktop\1\]
134 | 2023-06-28 16:33:36 | 2023-06-28 16:33:32 | | | 99812/2 | My Computer\CLSID_Desktop\PWF-main [Desktop\1\]
135 | 2023-06-28 16:33:36 | 2023-06-28 16:33:36 | | | 99845/2 | My Computer\CLSID_Desktop\PWF-main [Desktop\1\]
136 | 2023-06-28 16:33:36 | 2023-06-28 16:33:34 | | | 99830/3 | My Computer\CLSID_Desktop\PWF-main [Desktop\1\]
137 | 2023-06-28 17:45:00 | 2023-06-28 17:45:00 | | | 99852/3 | My Computer\CLSID_Desktop\PWF-main [Desktop\1\]
138 | 2023-06-28 16:33:36 | 2023-06-28 15:27:16 | | | | | My Computer\CLSID_Desktop\PWF-main [Desktop\1\]
139 | | | | | 2023-04-27 13:32:14 | | | | | My Computer\CLSID_Desktop\PWF-main [Desktop\1\]
140 | | | | | 2023-04-27 13:32:14 | | | | | My Computer\CLSID_Desktop\PWF-main [Desktop\1\]
141 | | | | | | | | | | | My Computer\C:\ [Desktop\1\3\]
142 | 2023-06-28 17:56:46 | 2023-06-28 16:42:32 | | | 99671/3 | My Computer\C:\AtomicRedTeam [Desktop\1\]
143 | 2023-06-28 17:57:04 | 2023-06-28 16:42:38 | | | 99737/4 | My Computer\C:\AtomicRedTeam\invoice [Desktop\1\]
144 | 2023-06-28 17:57:04 | 2023-06-28 16:42:38 | | | 99868/3 | My Computer\C:\AtomicRedTeam\invoice [Desktop\1\]
145 | 2023-06-28 17:57:04 | 2023-06-28 16:42:38 | | | 100972/4 | My Computer\C:\AtomicRedTeam\invoice [Desktop\1\]
146 | 2023-06-28 17:57:16 | 2023-06-28 17:57:08 | | | 104667/10 | My Computer\C:\AtomicRedTeam\invoice [Desktop\1\]
147 | 2023-06-29 08:01:18 | 2019-12-07 09:14:54 | | | 60/1 | My Computer\C:\Program Files [Desktop\1\]
148 | 2023-06-29 08:09:56 | 2023-06-28 16:30:32 | | | 102703/2 | My Computer\C:\Program Files\Oracle [Desktop\1\]
149 | 2023-06-29 08:09:50 | 2023-06-28 16:30:32 | | | 102704/2 | My Computer\C:\Program Files\Oracle [Desktop\1\]
150 | 2023-06-29 08:01:18 | 2019-12-07 09:14:54 | | | 1223/1 | My Computer\C:\Program Files (x86) [Desktop\1\]
151 | 2023-06-28 16:33:22 | 2023-06-28 15:27:16 | | | | | PWF-main.zip [2610224] [Desktop\2\]
152 | | | | | 2023-04-27 13:32:14 | | | | | PWF-main.zip\PWF-main [Desktop\2\]
153 | | | | | 2023-04-27 13:32:14 | | | | | PWF-main.zip\PWF-main\Install-Sysmon [Desktop\2\]
154 | 2023-06-28 16:33:32 | 2023-06-28 16:33:32 | | | 99809/3 | PWF-main [Desktop\3\]
155 | 2023-06-28 17:39:22 | 2023-06-28 16:33:32 | | | 99812/2 | PWF-main\PWF-main [Desktop\3\0\]
156 | 2023-06-28 17:45:00 | 2023-06-28 17:45:00 | | | 99835/3 | PWF-main\PWF-main\Install-Sysmon [Desktop\3\0\]
```

Normal text file length : 14,338 lines : 163 Ln : 1 Col : 1 Pos : 1 Windows (CR LF) UTF-8 INS

Usrclass.txt file edit with Notepad++.

C:\Cases\Analysis\Registry\UsrClass.dat.txt - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

all x DEFUALT.txt x NTUSER.DAT.txt x SECURITY.txt x SYSTEM.txt x SOFTWARE.txt x SAM.txt x UsrClass.dat.txt x

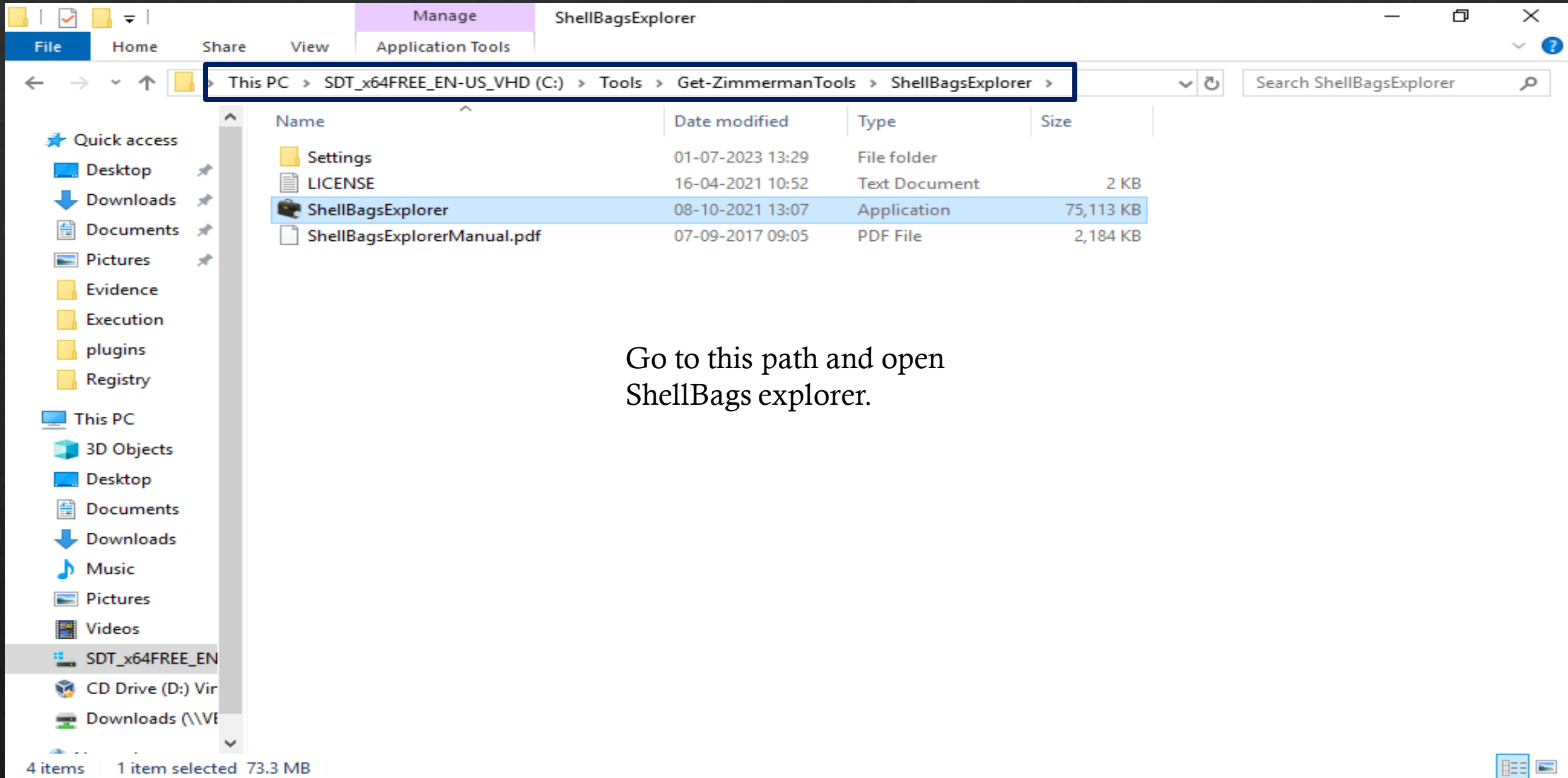
(USRCLASS.DAT) Shell/BagMRU traversal in Win7+ USRCLASS.DAT hives

MRU Time	Modified	Accessed	Created	Zip_Subfolder	MFT
2023-06-29 08:12:06					
2023-06-28 16:50:50	2023-06-28 16:33:32	2023-06-28 16:33:34	2023-06-28 16:33:32		9980
2023-06-28 16:33:44	2023-06-28 16:33:36	2023-06-28 16:33:36	2023-06-28 16:33:32		9981
	2023-06-28 16:33:36	2023-06-28 16:33:36	2023-06-28 16:33:36		9984
2023-06-28 17:56:18	2023-06-28 16:33:36	2023-06-28 16:33:36	2023-06-28 16:33:34		9983
	2023-06-28 17:45:00	2023-06-28 17:45:00	2023-06-28 17:45:00		9985
	2023-06-28 15:27:30	2023-06-28 16:33:36	2023-06-28 15:27:16		
2023-06-28 16:49:10				2023-04-27 13:32:14	
2023-06-28 16:49:53				2023-04-27 13:32:14	
2023-06-29 08:11:52					
	2023-06-28 17:56:46	2023-06-28 17:56:46	2023-06-28 16:42:32		9967
	2023-06-28 16:42:38	2023-06-28 17:57:04	2023-06-28 16:42:38		9973
	2023-06-28 16:42:38	2023-06-28 17:57:04	2023-06-28 16:42:38		9986
2023-06-28 17:57:29	2023-06-28 16:42:38	2023-06-28 17:57:04	2023-06-28 16:42:38		1009
2023-06-28 18:06:27	2023-06-28 17:57:16	2023-06-28 17:57:16	2023-06-28 17:57:08		1046
	2023-06-28 16:30:32	2023-06-29 08:01:18	2019-12-07 09:14:54		60/1
2023-06-29 08:11:56	2023-06-28 16:30:32	2023-06-29 08:09:56	2023-06-28 16:30:32		1027
2023-06-29 08:11:58	2023-06-28 16:30:54	2023-06-29 08:09:50	2023-06-28 16:30:32		1027
2023-06-29 08:12:06	2021-10-06 13:59:00	2023-06-29 08:01:18	2019-12-07 09:14:54		1223
	2023-06-28 15:27:30	2023-06-28 16:33:22	2023-06-28 15:27:16		
2023-06-28 16:48:32				2023-04-27 13:32:14	
2023-06-28 16:48:55				2023-04-27 13:32:14	

Normal text file length : 14,338 lines : 163 Ln : 1 Col : 1 Pos : 1 Windows (CR LF) UTF-8 INS

11:03 01-07-2023

Open the ShellBagsExplorer



Go to this path and open ShellBags explorer.

Insert the UsrClass.dat

The screenshot shows the ShellBags Explorer v1.4.0 application. A dialog box titled "Select a registry hive to open. Hold SHIFT to ignore dirty Registry hives" is open, displaying a file explorer view of the Registry folder. The file "UsrClass.dat" is selected and highlighted in blue. The "File name" field at the bottom of the dialog contains "UsrClass.dat". The "Open" button is highlighted with a blue border.

Name	Date modified	Type
NTUSER.DAT	29-06-2023 09:07	DAT File
NTUSER.DAT	01-07-2023 11:02	Text Document
SAM	29-06-2023 09:08	File
SAM	01-07-2023 10:55	Text Document
SECURITY	29-06-2023 09:08	File
SECURITY	01-07-2023 10:55	Text Document
SOFTWARE	29-06-2023 09:08	File
SOFTWARE	01-07-2023 10:55	Text Document
SYSTEM	29-06-2023 09:08	File
SYSTEM	01-07-2023 10:55	Text Document
UsrClass.dat	29-06-2023 09:07	DAT File
UsrClass.dat	01-07-2023 10:55	Text Document

File name: UsrClass.dat

Open Cancel

NA Time zone: UTC 0 of 0 visible 11:12 09-07-2023

Value
Desktop
My Computer
C:
Program Files (x86)
Program Files
AtomicRedTeam
Desktop
Z:
D:
Home Folder
PWF-main
PWF-main
PWF-main.zip
PWF-main

Drag a column header here to group by that column

	Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On
▼	ⓂC	No im...	ⓂC	=	=	=	=
	Home Folder	⚙️	Root folder: GUID	1			
	My Computer	⚙️	Root folder: GUID	0			
	PWF-main.zip	📄	File	3	2023-06-28 15:27:16	2023-06-28 15:27:30	2023-06-28 16:33:22
	PWF-main	📁	Directory	2	2023-06-28 16:33:32	2023-06-28 16:33:32	2023-06-28 16:33:32

Summary Details Hex

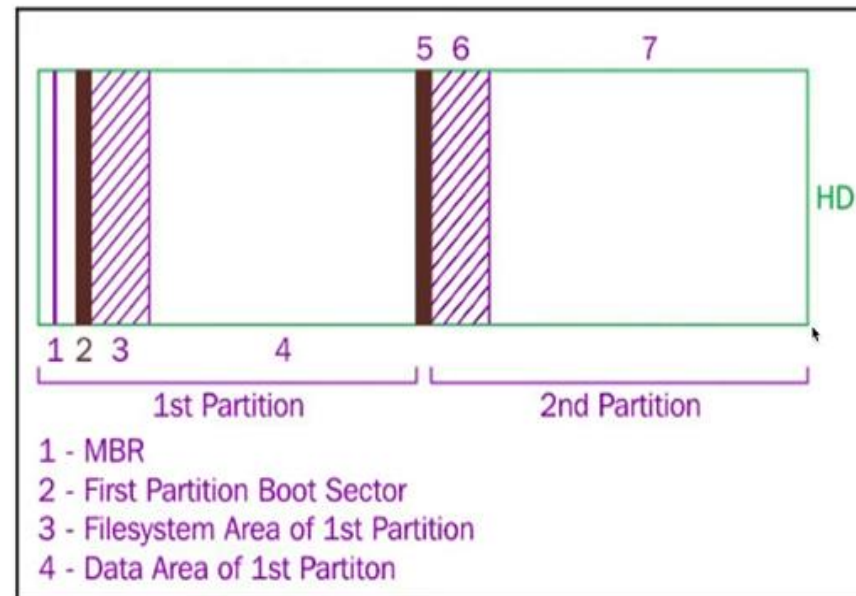
ShellBag items: 4

Show the output

NTFS- File system Analysis

NT file system (NTFS), which is also sometimes called the New Technology File System, is a process that the Windows NT operating system uses for storing, organizing, and finding files on a hard disk efficiently

Hard Disk Structure



Simple hard drive logical parts

MFT(Master File Table) records

Master File Table (MFT) MFT or \$MFT can be considered one of the most important files in the NTFS file system. It keeps records of all files in a volume, the files' location in the directory, the physical location of the files in on the drive, and file metadata.

Analysis of MFT Records with MFTECmd

The screenshot shows a Windows File Explorer window with the following details:

- Address bar: This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > F
- Left sidebar: Shows navigation pane with 'Cases' folder selected.
- Main pane: Displays a list of files and folders in the 'Cases' folder.

Name	Date modified	Type	Size
\$Extend	30-06-2023 08:31	File folder	
ProgramData	30-06-2023 08:30	File folder	
Users	30-06-2023 08:30	File folder	
Windows	30-06-2023 08:30	File folder	
\$Boot	30-06-2023 08:31	File	8 KB
\$LogFile	30-06-2023 08:31	File	65,536 KB
SMFT	29-06-2023 05:02	File	1,14,432 KB
\$Secure_\$SDS	29-06-2023 05:02	File	2,007 KB

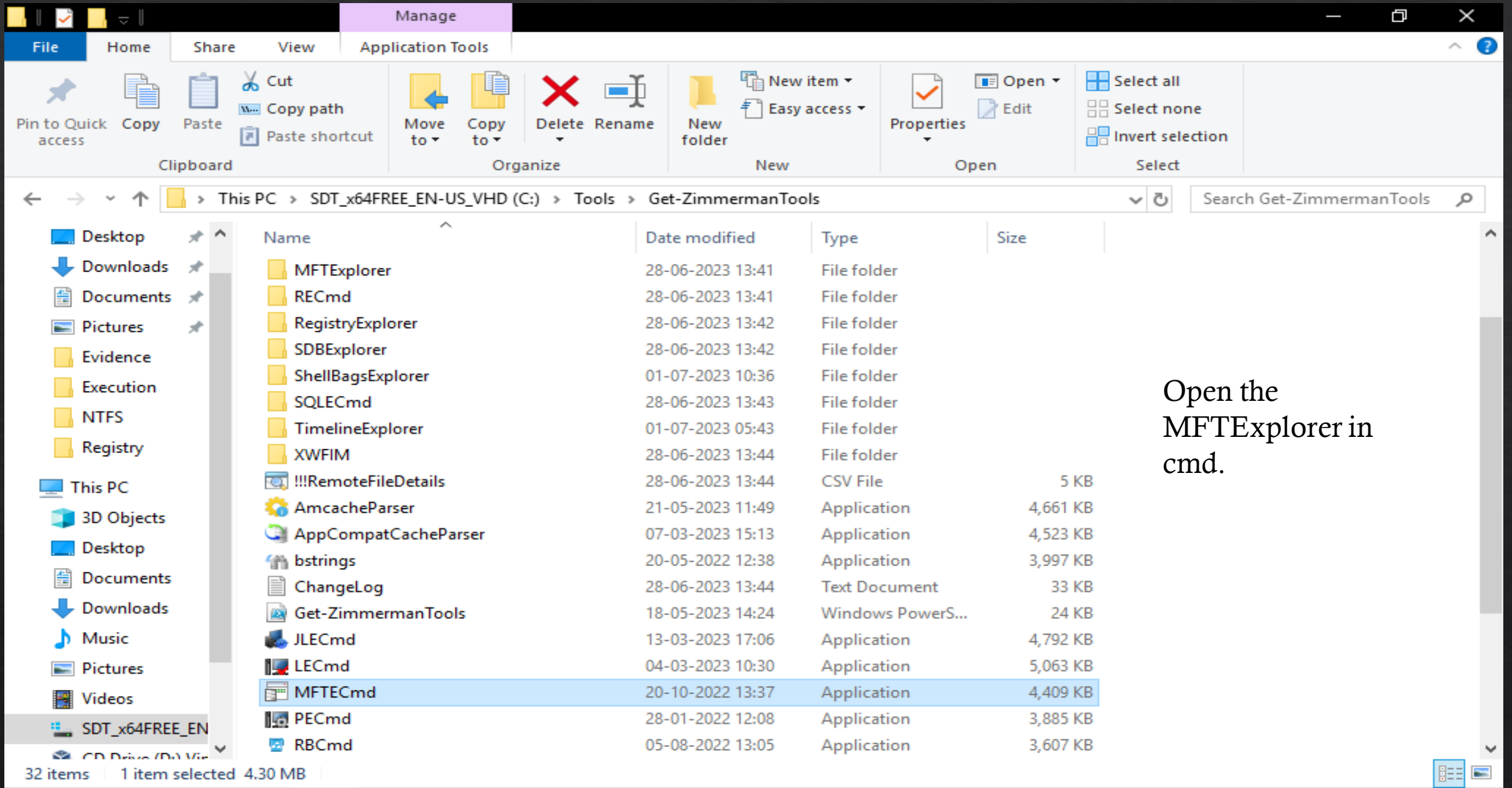
8 items | 1 item selected 111 MB

You can show MFT file in Cases folder. This file is use in MFT Records Analysis.



11:45
28-07-2023





Open the MFTEexplorer in cmd.

Name	Date modified	Type	Size
MFTEexplorer	28-06-2023 13:41	File folder	
RECcmd	28-06-2023 13:41	File folder	
RegistryExplorer	28-06-2023 13:42	File folder	
SDBExplorer	28-06-2023 13:42	File folder	
ShellBagsExplorer	01-07-2023 10:36	File folder	
SQLCcmd	28-06-2023 13:43	File folder	
TimelineExplorer	01-07-2023 05:43	File folder	
XWFIM	28-06-2023 13:44	File folder	
!!!RemoteFileDetails	28-06-2023 13:44	CSV File	5 KB
AmcacheParser	21-05-2023 11:49	Application	4,661 KB
AppCompatCacheParser	07-03-2023 15:13	Application	4,523 KB
bstrings	20-05-2022 12:38	Application	3,997 KB
ChangeLog	28-06-2023 13:44	Text Document	33 KB
Get-ZimmermanTools	18-05-2023 14:24	Windows PowerS...	24 KB
JLECcmd	13-03-2023 17:06	Application	4,792 KB
LECcmd	04-03-2023 10:30	Application	5,063 KB
MFTEcmd	20-10-2022 13:37	Application	4,409 KB
PECcmd	28-01-2022 12:08	Application	3,885 KB
RBCcmd	05-08-2022 13:05	Application	3,607 KB

32 items | 1 item selected 4.30 MB



Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Tools\Get-ZimmermanTools>MFTECmd.exe

Description:

MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)

<https://github.com/EricZimmerman/MFTECmd>

Examples: MFTECmd.exe -f "C:\Temp\SomeMFT" --csv "c:\temp\out" --csvf MyOutputFile.csv

MFTECmd.exe -f "C:\Temp\SomeMFT" --csv "c:\temp\out"

MFTECmd.exe -f "C:\Temp\SomeMFT" --json "c:\temp\jsonout"

MFTECmd.exe -f "C:\Temp\SomeMFT" --body "c:\temp\bout" --bdl c

MFTECmd.exe -f "C:\Temp\SomeMFT" --de 5-5

MFTECmd.exe -f "c:\temp\SomeJ" --csv c:\temp

MFTECmd.exe -f "c:\temp\SomeBoot"

MFTECmd.exe -f "c:\temp\SomeSecure_SDS" --csv c:\temp

MFTECmd.exe -f "c:\temp\SomeI30" --csv c:\temp

Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes

Usage:

MFTECmd [options]

Options:

- f <f> File to process (\$MFT | \$J | \$Boot | \$SDS | \$I30). Required
- m <m> \$MFT file to use when -f points to a \$J file (Use this to resolve parent path in \$J CSV output)
- json <json> Directory to save JSON formatted results to. This or --csv required unless --de or --body is specified
- jsonf <jsonf> File name to save JSON formatted results to. When present, overrides default name
- csv <csv> Directory to save CSV formatted results to. This or --json required unless --de or --body is specified
- csvf <csvf> File name to save CSV formatted results to. When present, overrides default name
- body <body> Directory to save bodyfile formatted results to. --bdl is also required when using this option
- bodyf <bodyf> File name to save body formatted results to. When present, overrides default name
- bdl <bdl> Drive letter (C, D, etc.) to use with bodyfile. Only the drive letter itself should be provided
- blf When true, use LF vs CRLF for newlines [default: False]

You can go in Get-ZimmermanTools path and open cmd and type this command for all helps




```
--csv <csv>      Directory to save CSV formatted results to. This or --json required unless --de or --body is
                 specified
--csvf <csvf>    File name to save CSV formatted results to. When present, overrides default name
--body <body>    Directory to save bodyfile formatted results to. --bdl is also required when using this option
--bodyf <bodyf>  File name to save body formatted results to. When present, overrides default name
--bdl <bdl>      Drive letter (C, D, etc.) to use with bodyfile. Only the drive letter itself should be provided
--blf           When true, use LF vs CRLF for newlines [default: False]
--dd <dd>       Directory to save exported $MFT FILE record. --do is also required when using this option
--do <do>       Offset of the $MFT FILE record to dump as decimal or hex. Ex: 5120 or 0x1400 Use --de or --debug to
                 see offsets
--de <de>       Dump full details for $MFT entry/sequence #. Format is 'Entry' or 'Entry-Seq' as decimal or hex.
                 Example: 5, 624-5 or 0x270-0x5.
--dr           When true, dump $MFT resident files to dir specified by --csv, in 'Resident' subdirectory. Files
                 will be named '<EntryNumber>-<SequenceNumber>_<FileName>.bin'
--fls          When true, displays contents of directory from $MFT specified by --de. Ignored when --de points to a
                 file [default: False]
--ds <ds>       Dump full details for Security Id from $SDS as decimal or hex. Example: 624 or 0x270
--dt <dt>       The custom date/time format to use when displaying time stamps. See https://goo.gl/CNVq0k for
                 options [default: yyyy-MM-dd HH:mm:ss.fffffff]
--sn          Include DOS file name types in $MFT output [default: False]
--fl          Generate condensed file listing of parsed $MFT contents. Requires --csv [default: False]
--at          When true, include all timestamps from 0x30 attribute vs only when they differ from 0x10 in the $MFT
                 [default: False]
--rs          When true, recover slack space from FILE records when processing $MFT files. This option has no
                 effect for $I30 files [default: False]
--vss         Process all Volume Shadow Copies that exist on drive specified by -f [default: False]
--dedupe      Deduplicate -f & VSCs based on SHA-1. First file found wins [default: False]
--debug       Show debug information during processing [default: False]
--trace       Show trace information during processing [default: False]
--version     Show version information
-?, -h, --help Show help and usage information
```

-f is required. Exiting

Show all option you can use in
Analysis.

C:\Tools\Get-ZimmermanTools>_



14:08
28-07-2023



```
C:\Tools\Get-ZimmermanTools>MFTECmd.exe -f c:\Cases\F\%MFT --de 0
MFTECmd version 1.2.2.1
```

```
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd
```

```
Command line: -f c:\Cases\F\%MFT --de 0
```

```
File type: Mft
```

```
Processed c:\Cases\F\%MFT in 21.7731 seconds
```

```
c:\Cases\F\%MFT: FILE records found: 1,12,778 (Free records: 1,394) File size: 111.8MB
```

```
Dumping details for file record with key 00000000-00000001
```

```
Entry-seq #: 0x0-0x1, Offset: 0x0, Flags: InUse, Log seq #: 0x1A155FD3, Base Record entry-seq: 0x0-0x0
Reference count: 0x1, FixUp Data Expected: 93-00, FixUp Data Actual: 00-00 | 00-00 (FixUp OK: True)
```

```
**** STANDARD INFO ****
```

```
Attribute #: 0x0, Size: 0x60, Content size: 0x48, Name size: 0x0, ContentOffset 0x18. Resident: True
Flags: Hidden, System, Max Version: 0x0, Flags 2: None, Class Id: 0x0, Owner Id: 0x0, Security Id: 0x100, Quota charged: 0x0, Update sequence #: 0x0
```

```
Created On:          2023-06-29 05:02:52.1527466
Modified On:         2023-06-29 05:02:52.1527466
Record Modified On: 2023-06-29 05:02:52.1527466
Last Accessed On:   2023-06-29 05:02:52.1527466
```

```
**** FILE NAME ****
```

```
Attribute #: 0x3, Size: 0x68, Content size: 0x4A, Name size: 0x0, ContentOffset 0x18. Resident: True
```

```
File name: %MFT
Flags: Hidden, System, Name Type: DosWindows, Reparse Value: 0x0, Physical Size: 0x4000, Logical Size: 0x4000
```

Using this command gathering the information about this file.



Last Accessed On: 2023-06-29 05:02:52.1527466

**** FILE NAME ****

Attribute #: 0x3, Size: 0x68, Content size: 0x4A, Name size: 0x0, ContentOffset 0x18. Resident: True

File name: \$MFT

Flags: Hidden, System, Name Type: DosWindows, Reparse Value: 0x0, Physical Size: 0x4000, Logical Size: 0x4000

Parent Entry-seq #: 0x5-0x5

Created On: 2023-06-29 05:02:52.1527466

Modified On: 2023-06-29 05:02:52.1527466

Record Modified On: 2023-06-29 05:02:52.1527466

Last Accessed On: 2023-06-29 05:02:52.1527466

**** DATA ****

Attribute #: 0x6, Size: 0x50, Content size: 0x0, Name size: 0x0, ContentOffset 0x0. Resident: False

Non-Resident Data

Starting Virtual Cluster #: 0x0, Ending Virtual Cluster #: 0x6FBF, Allocated Size: 0x6FC0000, Actual Size: 0x6FC0000, Initialized Size: 0x6FC0000

DataRuns Entries (Cluster offset -> # of clusters)

0xC0000 -> 0x67C0

0x2886D0 -> 0x800

**** BITMAP ****

Attribute #: 0x5, Size: 0x48, Content size: 0x0, Name size: 0x0, ContentOffset 0x0. Resident: False

Non-Resident Data

Starting Virtual Cluster #: 0x0, Ending Virtual Cluster #: 0x4, Allocated Size: 0x5000, Actual Size: 0x4008, Initialized Size: 0x4008

DataRuns Entries (Cluster offset -> # of clusters)

0x7B048 -> 0x5

C:\Tools\Get-ZimmermanTools>



12:02

28-07-2023



MFT parsing and in-depth analysis with MFTECmd

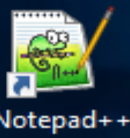
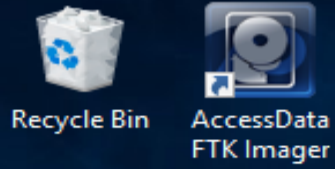
```
Administrator: C:\Windows\System32\cmd.exe
--ds <ds>      Dump full details for Security Id from $SDS as decimal or hex. Example: 624 or 0x270
--dt <dt>      The custom date/time format to use when displaying time stamps. See https://goo.gl/CNVq0k for
options [default: yyyy-MM-dd HH:mm:ss.fffffff]
--sn          Include DOS file name types in $MFT output [default: False]
--fl          Generate condensed file listing of parsed $MFT contents. Requires --csv [default: False]
--at          When true, include all timestamps from 0x30 attribute vs only when they differ from 0x10 in the $MFT
[default: False]
--rs          When true, recover slack space from FILE records when processing $MFT files. This option has no
effect for $I30 files [default: False]
--vss         Process all Volume Shadow Copies that exist on drive specified by -f [default: False]
--dedupe      Deduplicate -f & VSCs based on SHA-1. First file found wins [default: False]
--debug       Show debug information during processing [default: False]
--trace       Show trace information during processing [default: False]
--version     Show version information
-?, -h, --help Show help and usage information

-f is required. Exiting

C:\Tools\Get-ZimmermanTools>MFTECmd.exe -f c:\Cases\F\%MFT --csv c:\Cases\Analysis\NTFS --csvf MFT1.csv
MFTECmd version 1.2.2.1
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd
Command line: -f c:\Cases\F\%MFT --csv c:\Cases\Analysis\NTFS --csvf MFT1.csv
File type: Mft
Processed c:\Cases\F\%MFT in 11.7887 seconds
c:\Cases\F\%MFT: FILE records found: 1,12,778 (Free records: 1,394) File size: 111.8MB
CSV output will be saved to c:\Cases\Analysis\NTFS\MFT1.csv

C:\Tools\Get-ZimmermanTools>
```

Using this command all MFT file entry store in one file (MFT.csv) and then after show the details open using timeline explorer.



File Explorer window showing the NTFS folder structure. The left pane shows folders: Evidence, Execution, NTFS, Registry, This PC, 3D Objects, Desktop, Documents, Downloads. The right pane shows a table of files:

Name	Date modified	Type
MFT	01-07-2023 16:42	CSV File
MFT1	28-07-2023 14:19	CSV File

2 items | 1 item selected | 57.5 MB

Show the MFT1 file in NTFS folder and open with Timeline Explorer.

Drag a column header here to group by that column

PWF-main

Find

	In U...	Parent Path	File Name	Extensio
	<input type="checkbox"/>	ABC	ABC	ABC
3	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main	PWF-main	
4	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main	Investigation-roadmap.png	.png
4	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main	License.md	.md
4	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main	README.md	.md
4	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main	AtomicRedTeam	
3	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main\Atomic...	ART-attack-cleanup.ps1	.ps1
3	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main\Atomic...	ART-attack.ps1	.ps1
3	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main\Atomic...	PWF_Analysis-MITRE.png	.png
3	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main\Atomic...	PWF_Analysis-MITRE.svg	.svg
4	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main	Install-Sysmon	
3	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main\Instal...	Install-Sysmon.ps1	.ps1
4	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main	Resources	
3	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main\Resour...	Analysis-Notes-Template.docx	.docx
3	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main\Resour...	PracticalWindowsForensics-cheat-sheet.pdf	.pdf
3	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main\Resour...	Analysis-Notes-Template.docx	.docx
3	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main\Resour...	PracticalWindowsForensics-cheat-sheet.pdf	.pdf
3	<input checked="" type="checkbox"/>	.\Users\Denisha\Desktop\PWF-main\PWF-main\Resour...	RegRipper-plugins.csv	.csv

You can show any malicious activity and show detail, Here we find PWF-main script because this is run on target system.

MFT1.csv

Drag a column header here to group by that column

PWF-main

Find

	File Size	Created0x10	Created0x30	Last Modified0x10	Last Modified0x30	Last Record Change0x10
Y	=	=	=	=	=	=
	0	2023-06-28 17:44:57		2023-06-28 17:44...	2023-06-28 17:44:57	2023-06-28 17:44:58
	77340	2023-04-27 08:02:14	2023-06-28 17:44...	2023-04-27 08:02...	2023-06-28 17:44:57	2023-06-28 17:44:57
	34523	2023-04-27 08:02:14	2023-06-28 17:44...	2023-04-27 08:02...	2023-06-28 17:44:57	2023-06-28 17:44:57
	8345	2023-04-27 08:02:14	2023-06-28 17:44...	2023-04-27 08:02...	2023-06-28 17:44:57	2023-06-28 17:44:57
	0	2023-06-28 17:44:57		2023-06-28 17:44...	2023-06-28 17:44:57	2023-06-28 17:56:29
	2635	2023-04-27 08:02:14	2023-06-28 17:44...	2023-04-27 08:02...	2023-06-28 17:44:57	2023-06-28 17:44:57
	3360	2023-04-27 08:02:14	2023-06-28 17:44...	2023-04-27 08:02...	2023-06-28 17:44:57	2023-06-28 17:56:29
	234776	2023-04-27 08:02:14	2023-06-28 17:44...	2023-04-27 08:02...	2023-06-28 17:44:58	2023-06-28 17:44:58
	113692	2023-04-27 08:02:14	2023-06-28 17:44...	2023-04-27 08:02...	2023-06-28 17:44:58	2023-06-28 17:44:58
	0	2023-06-28 17:44:58		2023-06-28 17:44...		2023-06-28 17:44:58
	2673	2023-04-27 08:02:14	2023-06-28 17:44...	2023-04-27 08:02...	2023-06-28 17:44:58	2023-06-28 17:44:58
	0	2023-06-28 17:44:58		2023-06-28 17:44...	2023-06-28 17:44:58	2023-06-28 17:52:33
	19183	2023-04-27 08:02:14	2023-06-28 17:44...	2023-04-27 08:02...	2023-06-28 17:44:58	2023-06-28 17:44:58
	2979904	2023-04-27 08:02:14	2023-06-28 17:44...	2023-04-27 08:02...	2023-06-28 17:44:58	2023-06-28 17:52:33
	18374	2023-04-27 08:02:14	2023-06-28 17:44...	2023-04-27 08:02...	2023-06-28 17:44:58	2023-06-28 17:44:58
	22398	2023-04-27 08:02:14	2023-06-28 17:44...	2023-04-27 08:02...	2023-06-28 17:44:58	2023-06-28 17:44:58
	2610224	2023-06-28 17:44:42		2023-06-28 17:43...	2023-06-28 17:44:42	2023-06-28 17:43:34

MACB Timestamps Analysis

M – Modify

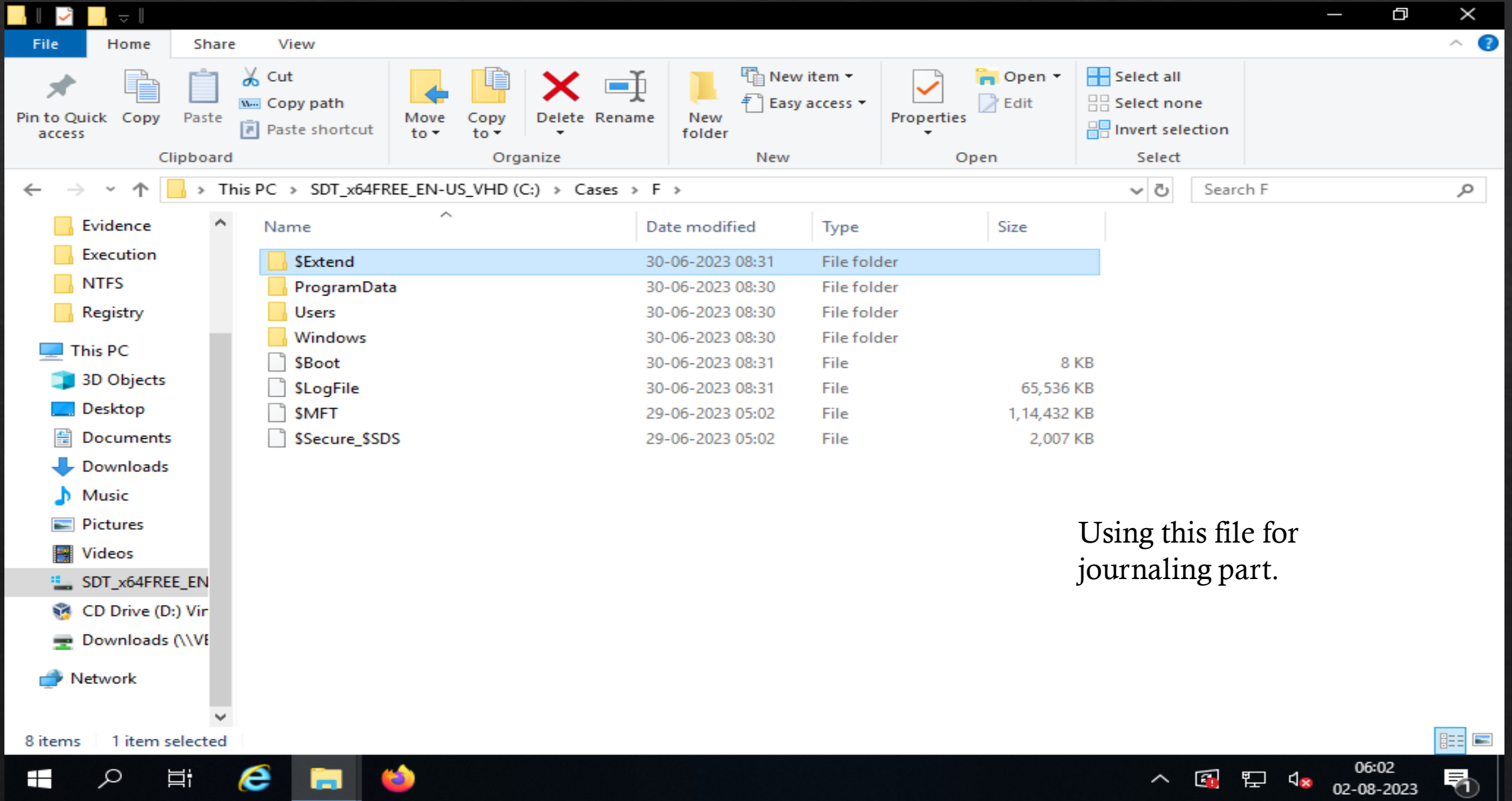
A – Access

C – Changed (last Access \$MFT)

B - (Birth) / Creation

You can Analysis MFT file so all timestamps are show you like all modifying time ,Access time, creation time, last Access time are known as MACB.

Finding Evidence of deleted files with USN Journal analysis



The screenshot shows a Windows File Explorer window with the following details:

- Path:** This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > F
- Left Navigation Pane:** Evidence, Execution, NTFS, Registry, This PC, 3D Objects, Desktop, Documents, Downloads, Music, Pictures, Videos, SDT_x64FREE_EN (selected), CD Drive (D:) Vir, Downloads (\\V), Network.
- Table of Contents:**

Name	Date modified	Type	Size
\$Extend	30-06-2023 08:31	File folder	
ProgramData	30-06-2023 08:30	File folder	
Users	30-06-2023 08:30	File folder	
Windows	30-06-2023 08:30	File folder	
\$Boot	30-06-2023 08:31	File	8 KB
\$LogFile	30-06-2023 08:31	File	65,536 KB
\$MFT	29-06-2023 05:02	File	1,14,432 KB
\$Secure_\$SDS	29-06-2023 05:02	File	2,007 KB

Using this file for journaling part.

File Explorer window titled "Get-ZimmermanTools" showing the contents of the "cmd" folder. The window includes a ribbon with "File", "Home", "Share", "View", and "Application Tools" tabs. The left sidebar shows navigation options like "This PC", "3D Objects", "Desktop", "Documents", "Downloads", "Music", "Pictures", "Videos", "SDT_x64FREE_EN", "CD Drive (D:) Vir", "System Reserved", "Local Disk (F:)", "Local Disk (G:)", "Downloads (\\V", and "Network".

The main pane displays a list of files and folders:

Name	Modified	Type	Size
cmd			
Search for "cmd"			
EZViewer	28-06-2023 13:40	File folder	
Hasher	28-06-2023 13:41	File folder	
iisGeolocate	28-06-2023 13:44	File folder	
JumpListExplorer	28-06-2023 13:41	File folder	
MFTEExplorer	28-06-2023 13:41	File folder	
RECcmd	28-06-2023 13:41	File folder	
RegistryExplorer	28-06-2023 13:42	File folder	
SDBExplorer	28-06-2023 13:42	File folder	
ShellBagsExplorer	01-07-2023 10:36	File folder	
SOLECmd	28-06-2023 13:43	File folder	
TimelineExplorer	01-07-2023 05:43	File folder	
XWFIM	28-06-2023 13:44	File folder	
!!!RemoteFileDetails	28-06-2023 13:44	CSV File	5 KB
AmcacheParser	21-05-2023 11:49	Application	4,661 KB
AppCompatCacheParser	07-03-2023 15:13	Application	4,523 KB
bstrings	20-05-2022 12:38	Application	3,997 KB
ChangeLog	28-06-2023 13:44	Text Document	33 KB
Get-ZimmermanTools	18-05-2023 14:24	Windows PowerS...	24 KB
JLECmd	13-03-2023 17:06	Application	4,792 KB
LECmd	04-03-2023 10:30	Application	5,063 KB
MFTECmd	20-10-2022 13:37	Application	4,409 KB
PECmd	28-01-2022 12:08	Application	3,885 KB

At the bottom, it shows "32 items | 1 item selected 4.30 MB".

MFTFcmd open

MFTECmd [options]

Options:

-f <f> File to process (\$MFT | \$J | \$Boot | \$SDS | \$I30). Required

-m <m> \$MFT file to use when -f points to a \$J file (Use this to resolve parent path in \$J CSV output)

--json <json> Directory to save JSON formatted results to. This or --csv required unless --de or --body is specified

--jsonf <jsonf> File name to save JSON formatted results to. When present, overrides default name

--csv <csv> Directory to save CSV formatted results to. This or --json required unless --de or --body is specified

--csvf <csvf> File name to save CSV formatted results to. When present, overrides default name

--body <body> Directory to save bodyfile formatted results to. --bdl is also required when using this option

--bodyf <bodyf> File name to save body formatted results to. When present, overrides default name

--bdl <bdl> Drive letter (C, D, etc.) to use with bodyfile. Only the drive letter itself should be provided

--blf When true, use LF vs CRLF for newlines [default: False]

--dd <dd> Directory to save exported \$MFT FILE record. --do is also required when using this option

--do <do> Offset of the \$MFT FILE record to dump as decimal or hex. Ex: 5120 or 0x1400 Use --de or --debug to see offsets

--de <de> Dump full details for \$MFT entry/sequence #. Format is 'Entry' or 'Entry-Seq' as decimal or hex. Example: 5, 624-5 or 0x270-0x5.

--dr When true, dump \$MFT resident files to dir specified by --csv, in 'Resident' subdirectory. Files will be named '<EntryNumber>-<SequenceNumber>_<FileName>.bin'

--fls When true, displays contents of directory from \$MFT specified by --de. Ignored when --de points to a file [default: False]

--ds <ds> Dump full details for Security Id from \$SDS as decimal or hex. Example: 624 or 0x270

--dt <dt> The custom date/time format to use when displaying time stamps. See <https://goo.gl/CNVq0k> for options [default: yyyy-MM-dd HH:mm:ss.fffffff]

--sn Include DOS file name types in \$MFT output [default: False]

--fl Generate condensed file listing of parsed \$MFT contents. Requires --csv [default: False]

--at When true, include all timestamps from 0x30 attribute vs only when they differ from 0x10 in the \$MFT [default: False]

--rs When true, recover slack space from FILE records when processing \$MFT files. This option has no effect for \$I30 files [default: False]

--vss Process all Volume Shadow Copies that exist on drive specified by -f [default: False]

--dedupe Deduplicate -f & VSCs based on SHA-1. First file found wins [default: False]

--debug Show debug information during processing [default: False]

--trace Show trace information during processing [default: False]



12:28

09-07-2023



Administrator: C:\Windows\System32\cmd.exe

```
--dedupe      Deduplicate -f & VSCs based on SHA-1. First file found wins [default: False]
--debug       Show debug information during processing [default: False]
--trace       Show trace information during processing [default: False]
--version     Show version information
-?, -h, --help Show help and usage information
```

-f is required. Exiting

```
C:\Tools\Get-ZimmermanTools>MFTECmd.exe -f C:\Cases\F\%Extend%\$J -m C:\Cases\F\%MFT --csv C:\Cases\Analysis\NTFS1
MFTECmd version 1.2.2.1
```

```
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd
```

```
Command line: -f C:\Cases\F\%Extend%\$J -m C:\Cases\F\%MFT --csv C:\Cases\Analysis\NTFS1
```

```
File type: UsnJournal
```

```
Processed C:\Cases\F\%MFT in 8.5757 seconds
```

```
C:\Cases\F\%MFT: FILE records found: 1,12,778 (Free records: 1,394) File size: 111.8MB
```

```
Path to C:\Cases\Analysis\NTFS1 doesn't exist. Creating...
```

```
CSV output will be saved to C:\Cases\Analysis\NTFS1\20230709123220_MFTECmd_%MFT_Output.csv
```

```
Processed C:\Cases\F\%Extend%\$J in 7.9542 seconds
```

```
Usn entries found in C:\Cases\F\%Extend%\$J: 2,43,185
```

```
CSV output will be saved to C:\Cases\Analysis\NTFS1\20230709123240_MFTECmd_%J_Output.csv
```

```
C:\Tools\Get-ZimmermanTools>_
```

Using this command use for store the all journal file in one folder.



12:33
09-07-2023



File Explorer window showing the contents of the NTFS1 folder. The path is: This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > Analysis > NTFS1. The folder contains two CSV files:

Name	Date modified	Type	Size
20230709123220_MFTECmd_\$MFT_Output	09-07-2023 12:32	CSV File	58,903 KB
20230709123240_MFTECmd_\$J_Output	09-07-2023 12:32	CSV File	50,449 KB

2 items | 1 item selected 49.2 MB

Show the Two file auto created and gather the information deleted file.

Drag a column header here to group by that column

Enter text to search...

Find

r	Parent Sequence Number	Update Sequence Number	Update Reasons	File A
▼	=	=	ABC	ABC ▲
761	1	22959408	HardLinkChange Close	Arct
761	1	22959536	HardLinkChange Close	Arct
761	1	22959664	HardLinkChange Close	Arct
761	1	22959792	HardLinkChange Close	Arct
761	1	22959920	HardLinkChange Close	Arct
761	1	22960048	FileDelete Close	Arct
761	1	22960176	FileDelete Close	Arct
761	1	22960304	FileDelete Close	Arct
761	1	22960432	FileDelete Close	Arct
761	1	22960560	FileDelete Close	Arct
761	1	22960688	HardLinkChange Close	Arct
761	1	22960824	FileDelete Close	Arct
761	1	22961000	FileDelete Close	Arct
761	1	22961168	HardLinkChange Close	Arct
761	1	22961304	FileDelete Close	Arct
761	1	22961480	FileDelete Close	Arct
761	1	22961648	HardLinkChange Close	Arct ▼



Evidence of Execution

1. BAM (Background Activity Moderator)

The screenshot shows two windows side-by-side. On the left is a Windows File Explorer window titled 'Registry' showing the contents of the 'SDT_x64FREE_EN-US' folder. The 'Registry' folder is selected. On the right is the 'Registry Explorer v1.6.0.0' application. The 'Registry hives (0)' section shows the 'SYSTEM' hive loaded. The 'Values' section is empty, and a 'Please Wait' dialog box is overlaid on it. The dialog box contains the text 'Please Wait Loading ...'.

Load the system hive
in Registry Explorer

Enter text to search...

Find

Key name	# values
<ul style="list-style-type: none"> {4d36e972-e325-11ce-bfc1-08002be10318} {53f56307-b6bf-11d0-94f2-00a0c91efb8b} {6bdd1fc6-810f-11d0-bec7-08002be2092f} AppCompatCache bam State <ul style="list-style-type: none"> UserSettings <ul style="list-style-type: none"> S-1-5-18 	=

Bookmark information

Hive:

Category:

Name:

Key path:

Short description:

Long description:

Drag a column header here to group by that column

Program	Execution Time
Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy	2023-06-28 18:13:52
MicrosoftWindows.Client.CBS_cw5n1h2txyewy	2023-06-28 18:13:50
\Device\HarddiskVolume2\Windows\System32\ApplicationFrameHost.exe	2023-06-29 09:07:46
windows.immersivecontrolpanel_cw5n1h2txyewy	2023-06-28 18:13:50
Microsoft.Windows.SecHealthUI_cw5n1h2txyewy	2023-06-28 16:47:51
Microsoft.XboxGamingOverlay_8wekyb3d8bbwe	2023-06-28 16:32:42
\Device\HarddiskVolume2\Windows\System32\cmd.exe	2023-06-28 16:32:49
\Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	2023-06-29 08:05:08
Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe	2023-06-29 09:07:46
Microsoft.WindowsStore_8wekyb3d8bbwe	2023-06-29 08:13:07
\Device\HarddiskVolume2\Windows\System32\notepad.exe	2023-06-28 17:58:27
\Device\HarddiskVolume2\Windows\System32\VBoxTray.exe	2023-06-29 09:07:43

Total rows: 17

Export ?

Type viewer

Value name:

Value type:

Key: ControlSet001\Services\bam\State\UserSettings\S-1-5-21-3331464962-214784631-3394824829-1001

Value: Version Collapse all hives

Selected hive: SYSTEM Last write: 29-06-2023 09:07:46 +00:00 19 of 19 values shown (100.00%)

Hidden keys: 0 1

Registry

File Home Share View

← → ↕ ↶ ↷ This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > Analysis > Registry Search Registry

Name	Date modified	Type	Size
UsrClass.dat	01-07-2023 10:55	Text Document	15 KB
UsrClass.dat	29-06-2023 09:07	DAT File	3,328 KB
SYSTEM	01-07-2023 10:55	Text Document	373 KB
SYSTEM	23 09:08	File	11,008 KB
SOFTWARE	23 10:55	Text Document	2,476 KB
SOFTWARE	23 09:08	File	68,608 KB
SECURITY	23 10:55	Text Document	4 KB
SECURITY	23 09:08	File	32 KB
SAM	23 10:55	Text Document	8 KB
SAM	23 09:08	File	64 KB
NTUSER	23 11:02	Text Document	39 KB
NTUSER	23 09:07	DAT File	1,024 KB
DEFAULT	23 10:55	Text Document	16 KB
DEFAULT	23 09:08	File	512 KB

Open
Print
Edit
Edit with Notepad++
Share
Open with >
Restore previous versions
Send to >
Cut
Copy
Create shortcut
Delete
Rename
Properties

14 items | 1 item selected 372 KB

System.txt file edit with Notepad++.

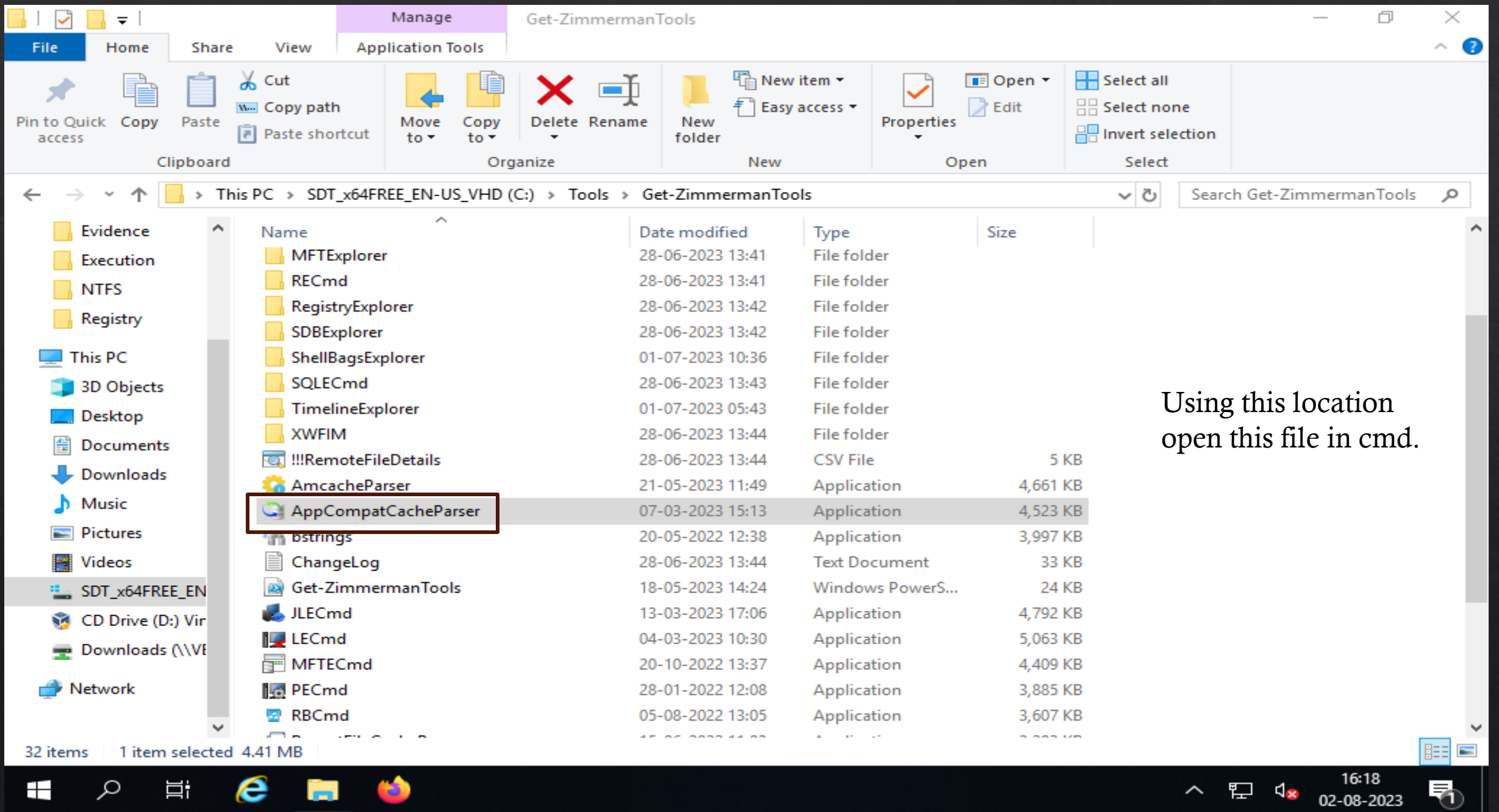
```
C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
all | DEFAULT.txt | NTUSER.DAT.txt | SECURITY.txt | SOFTWARE.txt | SAM.txt | UsrClass.dat.txt | SYSTEM.txt
424 Pending Rename Operations2 : CurrentControlSet\Control\Session Manager\PendingFileRenameOperations2
425 -----
426 bam v.20200427
427 (System) Parse files from System hive BAM Services
428
429 S-1-5-18
430 2023-06-28 16:23:05Z - \Device\HarddiskVolume2\Windows\System32\oobe\FirstLogonAnim.exe
431
432 S-1-5-21-3331464962-214784631-3394824829-1000
433 2023-06-28 16:20:23Z - \Device\HarddiskVolume2\Windows\explorer.exe
434 2023-06-28 16:20:23Z - Microsoft.Windows.CloudExperienceHost_cw5nlh2txyewy
435 2023-06-28 16:20:22Z - MicrosoftWindows.Client.CBS_cw5nlh2txyewy
436
437 S-1-5-21-3331464962-214784631-3394824829-1001
438 2023-06-29 09:07:45Z - \Device\HarddiskVolume2\Windows\explorer.exe
439 2023-06-29 09:07:46Z - Microsoft.Windows.StartMenuExperienceHost_cw5nlh2txyewy
440 2023-06-29 09:07:46Z - Microsoft.Windows.Search_cw5nlh2txyewy
441 2023-06-28 18:13:52Z - Microsoft.Windows.ShellExperienceHost_cw5nlh2txvewy
```

```
Search results - (12 hits)
Search "bam" (12 hits in 1 file of 1 searched)
C:\Cases\Analysis\Registry\SYSTEM.txt (12 hits)
Line 426: bam v.20200427
Line 427: (System) Parse files from System hive BAM Services
Line 1408: Name = bam
Line 1409: Display = @%SystemRoot%\system32\drivers\bam.sys,-100
Line 1410: ImagePath = system32\drivers\bam.sys
Line 5970: 2023-06-29 08:01:14Z,BasicDisplay,,\SystemRoot\System32\DriverStore\FileRepository\basicdisplay.inf_amd64_65e
Line 6000: 2023-06-29 08:00:59Z,BasicRender,,\SystemRoot\System32\DriverStore\FileRepository\basicrender.inf_amd64_df49c
Line 6050: 2023-06-28 16:04:29Z,bam,@%SystemRoot%\system32\drivers\bam.sys;-100,system32\drivers\bam.sys,Kernel driver,S
```

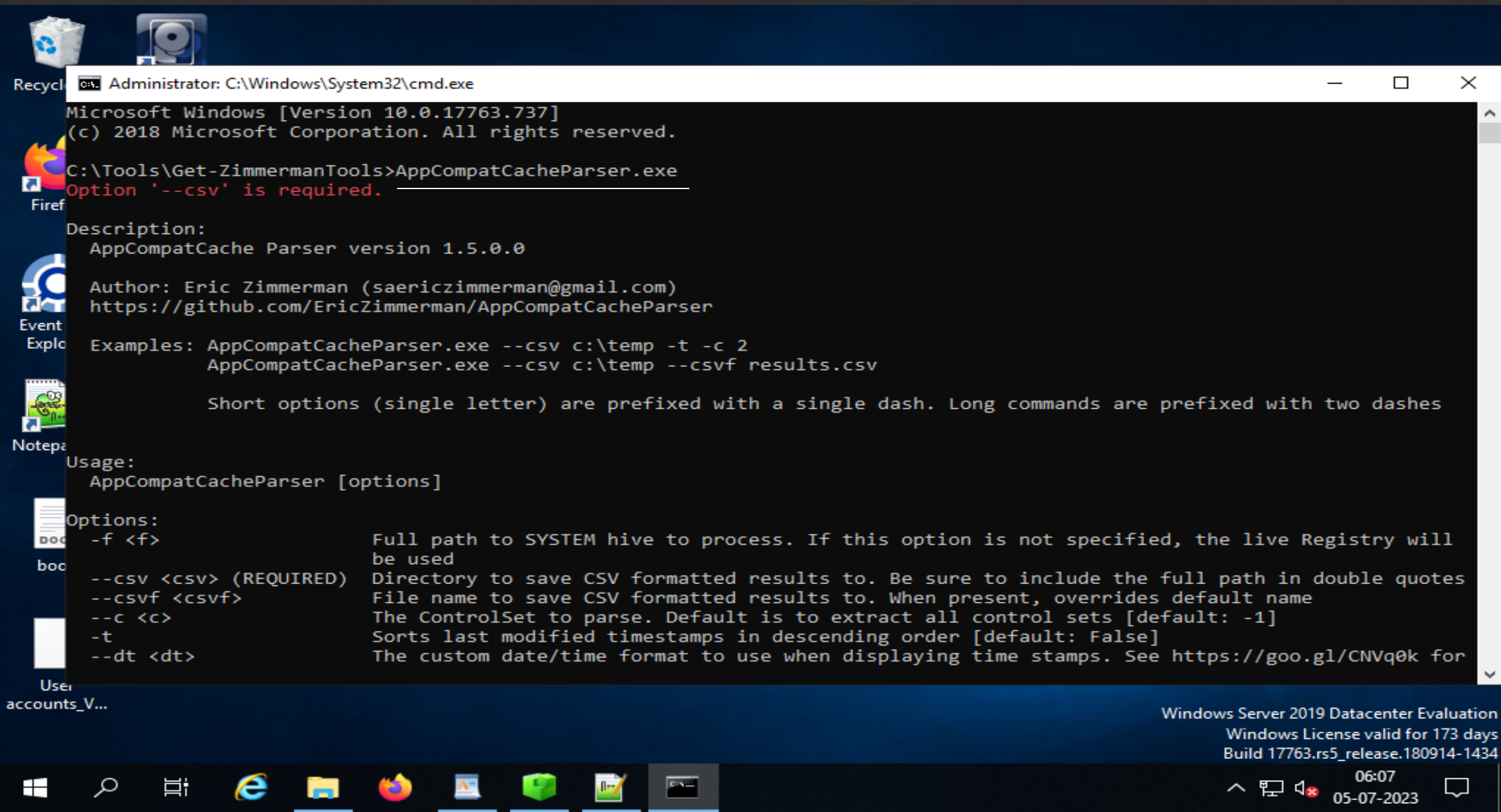
Normal text file | length: 3,81,631 lines: 7,241 | Ln: 427 Col: 1 Sel: 16 | 1 | Windows (CR LF) | UTF-8 | INS

2. AppCompactcache Analysis/Shimcache

The shimcache is a Windows registry entry that records metadata about executed applications, including timestamps and filenames.



Go to the Appcompatcacheparser.exe in cmd



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Tools\Get-ZimmermanTools>AppCompatCacheParser.exe
Option '--csv' is required.

Description:
AppCompatCache Parser version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AppCompatCacheParser

Examples: AppCompatCacheParser.exe --csv c:\temp -t -c 2
AppCompatCacheParser.exe --csv c:\temp --csvf results.csv

Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes

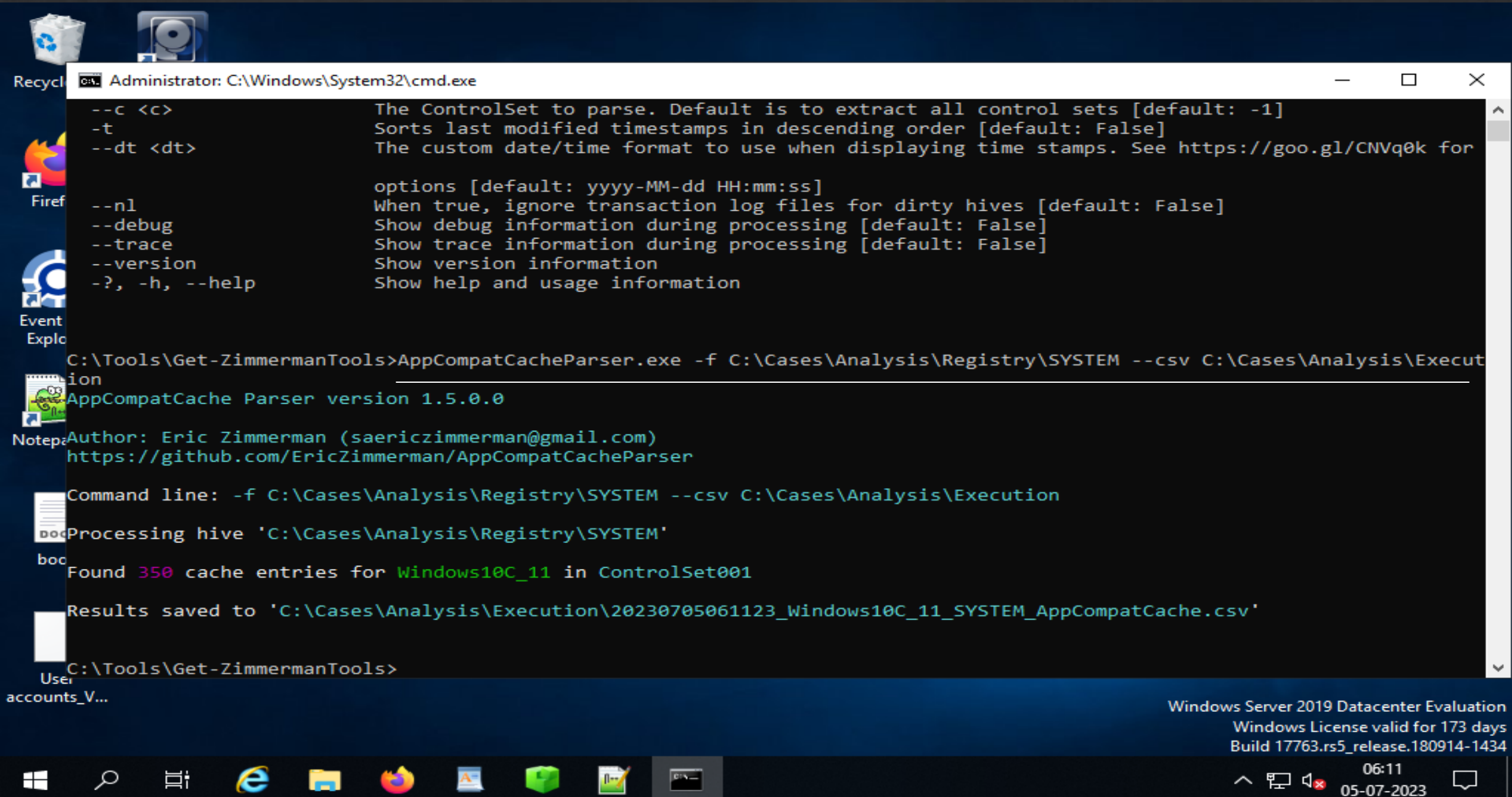
Usage:
AppCompatCacheParser [options]

Options:
-f <f>          Full path to SYSTEM hive to process. If this option is not specified, the live Registry will
                be used
--csv <csv> (REQUIRED) Directory to save CSV formatted results to. Be sure to include the full path in double quotes
--csvf <csvf>      File name to save CSV formatted results to. When present, overrides default name
--c <c>          The ControlSet to parse. Default is to extract all control sets [default: -1]
-t             Sorts last modified timestamps in descending order [default: False]
--dt <dt>       The custom date/time format to use when displaying time stamps. See https://goo.gl/CNVq0k for
```

Windows Server 2019 Datacenter Evaluation
Windows License valid for 173 days
Build 17763.rs5_release.180914-1434

06:07
05-07-2023

Create the folder Execution in Analysis and run this command and store the output in Execution folder.



```
Administrator: C:\Windows\System32\cmd.exe
--c <c>           The ControlSet to parse. Default is to extract all control sets [default: -1]
-t              Sorts last modified timestamps in descending order [default: False]
--dt <dt>       The custom date/time format to use when displaying time stamps. See https://goo.gl/CNVq0k for
                options [default: yyyy-MM-dd HH:mm:ss]
--nl           When true, ignore transaction log files for dirty hives [default: False]
--debug        Show debug information during processing [default: False]
--trace        Show trace information during processing [default: False]
--version      Show version information
-?, -h, --help Show help and usage information

C:\Tools\Get-ZimmermanTools>AppCompatCacheParser.exe -f C:\Cases\Analysis\Registry\SYSTEM --csv C:\Cases\Analysis\Execution
AppCompatCache Parser version 1.5.0.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AppCompatCacheParser

Command line: -f C:\Cases\Analysis\Registry\SYSTEM --csv C:\Cases\Analysis\Execution
Processing hive 'C:\Cases\Analysis\Registry\SYSTEM'
Found 350 cache entries for Windows10C_11 in ControlSet001
Results saved to 'C:\Cases\Analysis\Execution\20230705061123_Windows10C_11_SYSTEM_AppCompatCache.csv'

C:\Tools\Get-ZimmermanTools>
```

Windows Server 2019 Datacenter Evaluation
Windows License valid for 173 days
Build 17763.rs5_release.180914-1434
06:11
05-07-2023



File Explorer window showing the path: < Cases > Analysis > Execution. The file list contains one item:

Name	Date modified	Type
20230705061123_Windows10C_11_SYSTE...	05-07-2023 06:11	CSV File

1 item

Show the file in Execution folder.

Output show in Timeline Explorer.

Drag a column header here to group by that column

Enter text to search...

Find

	Line	Tag	Control S...	Duplicate	Cache Entry Posi...	Executed	Last Modified Time UTC	Path
▼	=	<input checked="" type="checkbox"/>	=	<input checked="" type="checkbox"/>	=	RBc	=	RBc
▶	1	<input type="checkbox"/>	1	<input type="checkbox"/>	0	No	2021-10-06 13:52:38	C:\Windows\system32\sp
	2	<input type="checkbox"/>	1	<input type="checkbox"/>	1	No		00000009 000a564b27390
	3	<input type="checkbox"/>	1	<input type="checkbox"/>	2	No		00000009 000b08a200000
	4	<input type="checkbox"/>	1	<input type="checkbox"/>	3	No		00000009 00010000f0970
	5	<input type="checkbox"/>	1	<input type="checkbox"/>	4	No		00000009 000c005f0bb90
	6	<input type="checkbox"/>	1	<input type="checkbox"/>	5	No		00000009 000b08ff00050
	7	<input type="checkbox"/>	1	<input type="checkbox"/>	6	No	2023-06-29 08:25:43	C:\Program Files\Windo
	8	<input type="checkbox"/>	1	<input type="checkbox"/>	7	No		00000009 000f00630c820
	9	<input type="checkbox"/>	1	<input type="checkbox"/>	8	No		00000009 0012090104c60
	10	<input type="checkbox"/>	1	<input type="checkbox"/>	9	No	2023-06-29 08:13:18	C:\ProgramData\Microso
	11	<input type="checkbox"/>	1	<input type="checkbox"/>	10	No	2023-06-29 08:24:59	C:\Program Files\Windo
	12	<input type="checkbox"/>	1	<input type="checkbox"/>	11	Yes		00000009 00015a0c00790
	13	<input type="checkbox"/>	1	<input type="checkbox"/>	12	No	2023-06-29 08:24:55	C:\Program Files\Windo
	14	<input type="checkbox"/>	1	<input type="checkbox"/>	13	No		00000009 000b090000000
	15	<input type="checkbox"/>	1	<input type="checkbox"/>	14	No		00000009 00015a0c00790
	16	<input type="checkbox"/>	1	<input type="checkbox"/>	15	No		00000009 0004089c33f70
	17	<input type="checkbox"/>	1	<input type="checkbox"/>	16	Yes		00000009 07e7272e697a0
	18	<input type="checkbox"/>	1	<input type="checkbox"/>	17	No	2023-06-29 08:22:37	C:\Program Files\Windo
	19	<input type="checkbox"/>	1	<input type="checkbox"/>	18	No		00000009 000b0900000020

C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

all x DEFUALT.txt x NTUSER.DAT.txt x SECURITY.txt x SOFTWARE.txt x SAM.txt x UsrClass.dat.txt x SYSTEM.txt x

```
10 appcompatcache v.20220921
11 (System) Parse files from System hive AppCompatCache
12
13 ControlSet001\Control\Session Manager\AppCompatCache
14 LastWrite Time: 2023-06-29 09:08:05Z
15 Signature: 0x34
16 SIGN.MEDIA=A1AA6D23 VirtualBox-7.0.8-156879-Win.exe 2023-06-26 05:56:58
17 00000000 0002a41723290000 000a000047ba0000 8664 Microsoft.UI.X
18 00000009 0005077207b40000 000a000045630000 8664 Microsoft.Wind
19 C:\Windows\system32\wevtutil.exe 2021-10-06 13:52:38
20 C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5nlh2txy
21 0000000b 03e84a6103ff0000 000a000000000000 8664 Microsoft.Wind
22 C:\Windows\system32\MusNotification.exe 2021-10-06 13:52:39
23 C:\Program Files\WindowsApps\Microsoft.XboxApp_48.49.31001.0_x64__8wekyb3d
24 C:\Windows\system32\wbem\wmiprvse.exe 2021-10-06 13:52:41
25 00000009 07e7272e697a0000 000a00004a640000 8664 Microsoft.Wind
26 00000009 000e00007f120000 000a0000273a0000 8664 Microsoft.VCLi
27 C:\Windows\Microsoft.NET\Framework\v4.0.30319\NGenTask.exe 2021-10-06 13:
28 C:\Program Files (x86)\Microsoft\EdgeUpdate\Install\{175CC469-9B9D-4132-9B
29 C:\Windows\system32\oobe\FirstLogonAnim.exe 2019-12-07 09:09:05
30 C:\Windows\System32\ mobsync.exe 2019-12-07 09:09:47
31 00000000 0002000273480000 000a000027410000 8664 Microsoft.NET.
32 C:\Windows\system32\SearchFilterHost.exe 2021-10-06 13:52:31
33 0000000b 000a00004a6103ff 000a00004a6103ff 8664 Microsoft.Windows.ShellExperienceHost cw5nlh2txyewy ne
34 C:\Windows\system32\osk.exe 2019-12-07 09:08:43
35 C:\Windows\system32\wbem\unsecapp.exe 2021-10-06 13:52:05
36 C:\Windows\system32\cleanmgr.exe 2021-10-06 13:53:34
37 00000009 3e8137f653cc0000 000a000047ba0000 8664 Microsoft.Office.OneNote 8wekyb3d8bbwe
38 00000009 000e00007f120000 000a0000273a0000 8664 Microsoft.VCLibs.140.00.UWPDesktop 8wekyb3d8bbwe
39 00000009 00015a0c00790000 000a00004a640000 8664 Microsoft.YourPhone 8wekyb3d8bbwe
```

Find

Find Replace Find in Files Find in Projects Mark

Find what: appcompatcache

In selection

Backward direction

Match whole word only

Match case

Wrap around

Search Mode

Normal

Extended (\n, \r, \t, \0, \x...)

Regular expression . matches newline

System hives edit with Notepad++

Normal text file length: 3,81,631 lines: 7,241 Ln: 10 Col: 15 Sel: 14 | 1 Windows (CR LF) UTF-8 INS

06:03 05-07-2023

3. Analyzing the Amcache with AmcacheParser

AmCache.hve is a Windows system file that is created to store information related to program executions. The artifacts in this file can serve as a huge aid in an investigation, it records the processes recently run on the system and lists the paths of the files executed.

Load the Amcache.hve on Registry Explorer

The screenshot shows a Windows File Explorer window displaying the file `Amcache.hve` (1,280 KB) in the path `C:\Cases\F\Windows\AppCompat\Programs`. Below it, the Registry Explorer v1.6.0.0 application is open, showing the registry tree with the key `C:\Cases\F\Windows\AppCompat\Programs\{11517B7C-...}` selected. The right pane shows the registry values for this key.

Value Name	Value Type	Data	Value Slack	Is Deleted
CreatingCommand	RegSz	"C:\Program File...	2D-00-32-00-44-...	<input type="checkbox"/>
CreatingModule	RegSz	C:\Windows\SYS...		<input type="checkbox"/>



16:38

09-07-2023



Enter text to search... Find

Key name	# values	# subkeys
C:\Cases\F\Windows\AppCo...	=	=
{11517B7C-E79D-4e20-961B-75...}	2	
Root	0	2
DeviceCensus	1	1
DriverPackageExtended	2	
InventoryApplication	24	8
InventoryApplicationAppv	1	
InventoryApplicationFile	2	12
3dviewer.exe 0b0cece...	19	
appinstaller.exe c736df...	19	
appinstallelev a8a669...	19	
appinstallerpyth 67732a...	19	
calculator.exe 724943cb...	19	
codecpacks.heif. 7deccd...	19	
codecpacks.vp9.e 86e4...	19	
codecpacks.webp. daa3...	19	
compattelrunner. 732ad...	20	
cookie_exporter. 21e69...	19	
cookie_exporter. 81014...	19	
cookie_exporter. c1715...	19	
cortana.exe d59b9eee1...	19	

Drag a column header here to group by that column

Timestamp	Path	Name	Product Name	Publisher	Version	SHA 1
2023-06-29 0...	c:\program files\windowsap ps\microsoft.mi crosoft3dviewe r_6.1908.2042. 0_x64__8weky b3d8bbwe\3dvi ewer.exe	3DViewer.exe	view 3d	microsoft corporation	6.1908.2042.0	ee05f81b330d2e755d8028ec5da859cf9eae1813
2023-06-29 0...	c:\program files\windowsap ps\microsoft.de sktopappinstall er_1.0.30251.0 _x64__8wekyb 3d8bbwe\appin staller.exe	AppInstaller.exe	microsoft appx click handler	microsoft corporation	1.0.1901.25001	828d5cf25052ad0686636867130f5a8ff4b71a83
2023-06-29 0...	c:\program files\windowsap ps\microsoft.de sktopappinstall er_1.0.30251.0 _x64__8wekyb 3d8bbwe\appin staller.exe	AppInstallerEle vatedAppServic eClient.exe	microsoft appx click handler	microsoft corporation	1.0.1901.25001	935407d4d0d898f997d5231daffa3329a1443f56

Total rows: 128 Export ?

Type viewer Binary viewer

Value name WritePermissionsCheck

Value type RegDword

Key: Root\InventoryApplicationFile Value: WritePermissionsCheck Collapse all hives

Selected hive: Amcache.hve Last write: 2023-06-29 08:12:32 2 of 2 values shown (100.00%) Load complete Hidden keys: 0 1

Manage Arsenal-Image-Mounter-v3.9.239

File Home Share View Application Tools

Arsenal Image Mounter

File BitLocker Advanced Help

+ Z:\Evidence\{0926ccea-dfd7-4e08-bd93-7a85bd797974}_copy.vhd
Mount Points: E:\, F:\, G:\

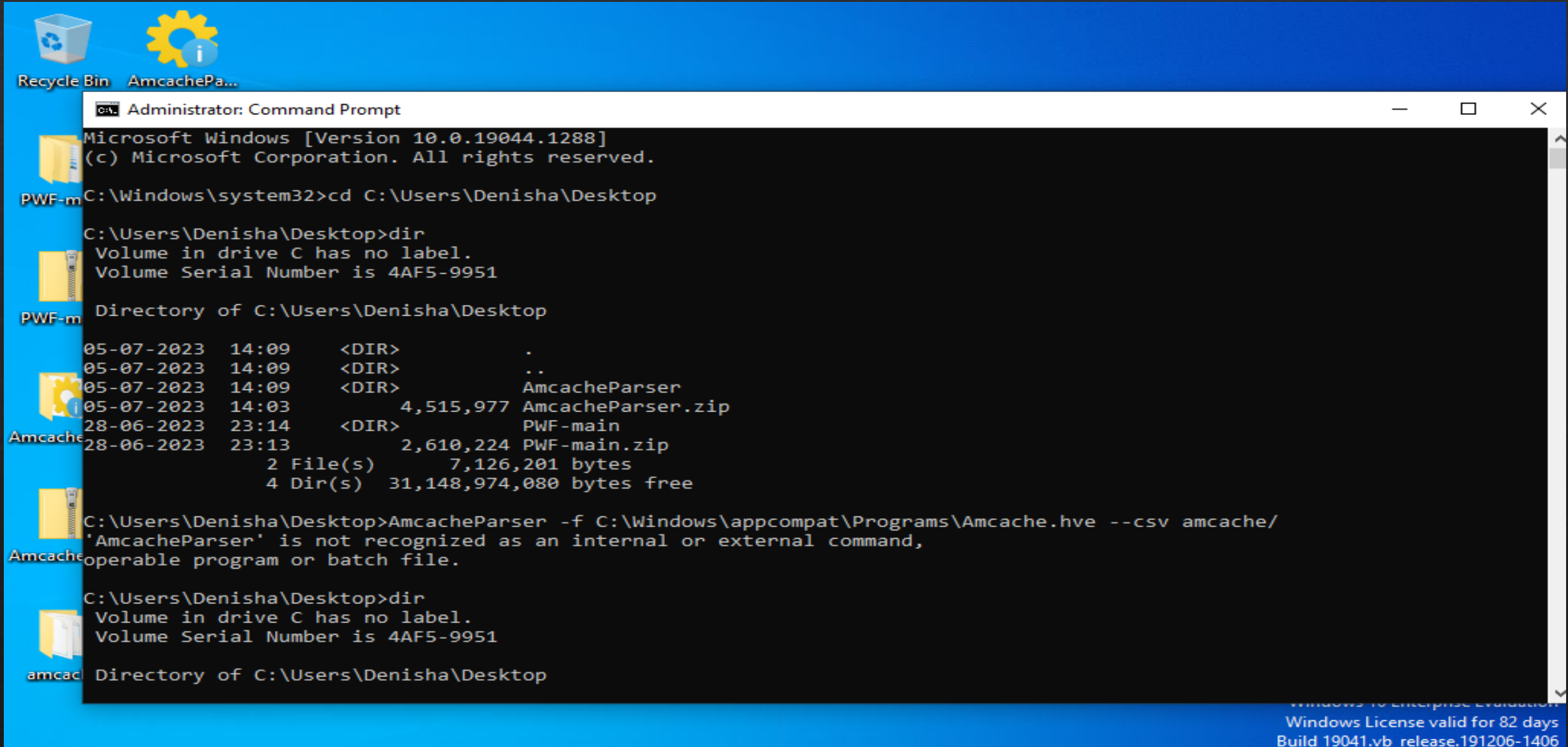
Launch VM feature
is disable

+ Mount disk image Mount VSCs Launch VM Remove Remove all Refresh

Local Disk (F:) DiscUtils.Lvm.dll 28-02-2023 17:04 Application extens... 43 KB

53 items 1 item selected 493 KB

Go to the target system and Download the Amcache in link <https://ericzimmerman.github.io/#!index.md> and open cmd with Run as a Administrator.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Denisha\Desktop

C:\Users\Denisha\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 4AF5-9951

Directory of C:\Users\Denisha\Desktop

05-07-2023  14:09    <DIR>          .
05-07-2023  14:09    <DIR>          ..
05-07-2023  14:09    <DIR>          AmcacheParser
05-07-2023  14:03             4,515,977 AmcacheParser.zip
28-06-2023  23:14    <DIR>          PWF-main
28-06-2023  23:13             2,610,224 PWF-main.zip
                2 File(s)      7,126,201 bytes
                4 Dir(s)  31,148,974,080 bytes free

C:\Users\Denisha\Desktop>AmcacheParser -f C:\Windows\appcompat\Programs\Amcache.hve --csv amcache/
'AmcacheParser' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Denisha\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 4AF5-9951

Directory of C:\Users\Denisha\Desktop
```

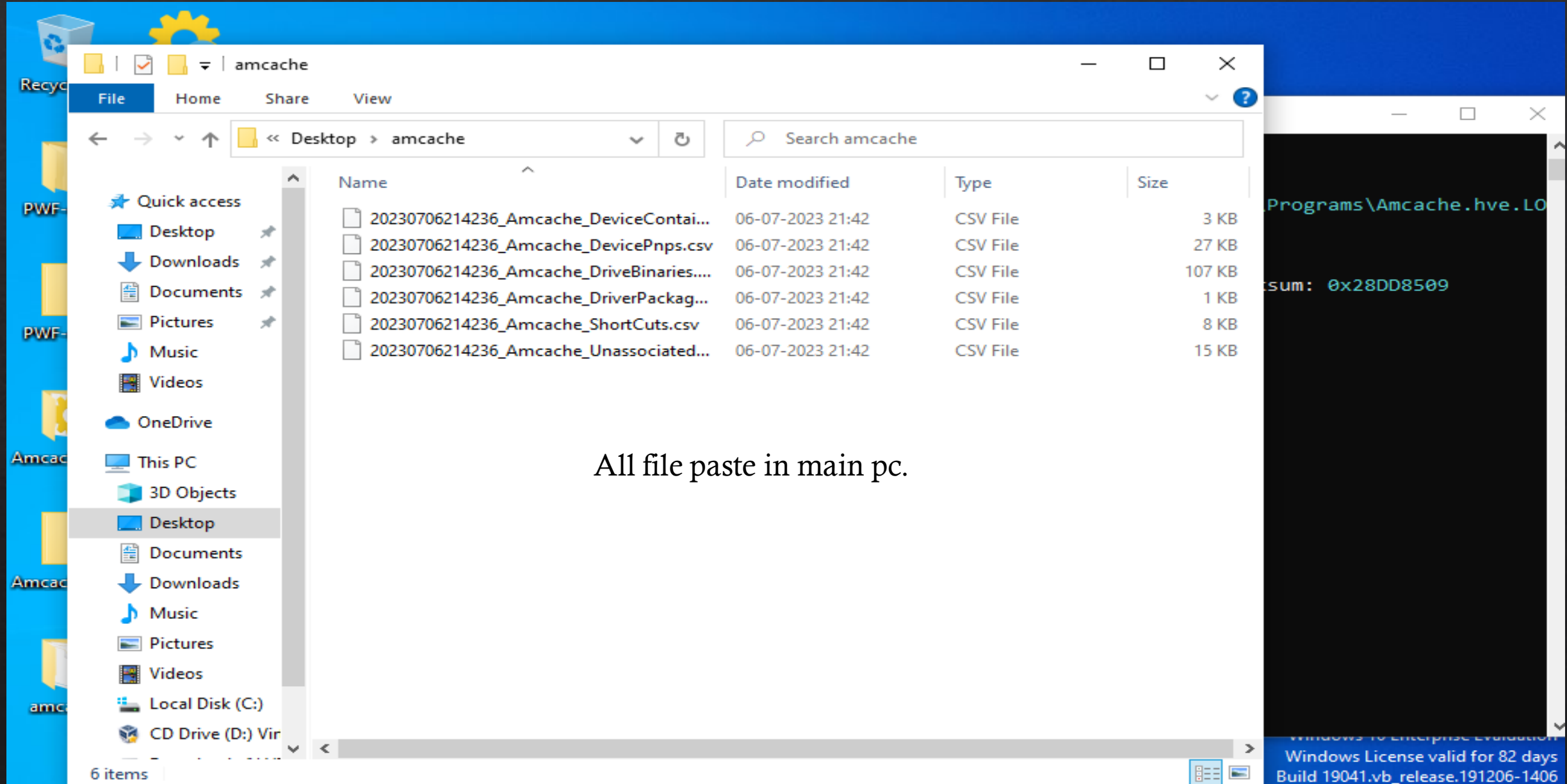
Windows 10 Enterprise Evaluation
Windows License valid for 82 days
Build 19041.vb_release.191206-1406



```
Administrator: Command Prompt
4 Dir(s) 31,229,493,248 bytes free
C:\Users\Denisha\Desktop>AmcacheParser.exe -f C:\Windows\appcompat\Programs\Amcache.hve --csv amcache/
AmcacheParser version 1.5.1.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AmcacheParser
Command line: -f C:\Windows\appcompat\Programs\Amcache.hve --csv amcache/
Two transaction logs found. Determining primary log...
Primary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG1, secondary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
At least one transaction log was applied. Sequence numbers have been updated to 0x002F. New Checksum: 0x28DD8509
'C:\Windows\appcompat\Programs\Amcache.hve' is in use. Rerouting...
Two transaction logs found. Determining primary log...
Primary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG1, secondary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
At least one transaction log was applied. Sequence numbers have been updated to 0x002F. New Checksum: 0x28DD8509
C:\Windows\appcompat\Programs\Amcache.hve is in new format!
Total file entries found: 131
Total shortcuts found: 50
Total device containers found: 9
```

Windows 10 Enterprise Evaluation
Windows License valid for 82 days
Build 19041.vb_release.191206-1406

All File create in Amcache folder. Amcache folder copy the main pc and open with excel and show the output.



All file paste in main pc.



Type here to search



27°C



ENG

21:48

06-07-2023



File Explorer window showing the contents of the 'amcache' folder in the 'Downloads' directory of 'This PC'. The address bar shows the path: This PC > Downloads > amcache. The search bar contains 'Search amcache'.

Name	Date modified	Type	Size
20230706214236_Amcache_DeviceContai...	06-07-2023 21:42	Microsoft Excel C...	3 KB
20230706214236_Amcache_DevicePnps	06-07-2023 21:42	Microsoft Excel C...	27 KB
20230706214236_Amcache_DriveBinaries	06-07-2023 21:42	Microsoft Excel C...	107 KB
20230706214236_Amcache_DriverPackages	06-07-2023 21:42	Microsoft Excel C...	1 KB
20230706214236_Amcache_ShortCuts	06-07-2023 21:42	Microsoft Excel C...	8 KB
20230706214236_Amcache_Unassociated...	06-07-2023 21:42	Microsoft Excel C...	15 KB

The file '20230706214236_Amcache_Unassociated...' is selected and highlighted in blue. An arrow points to this file from the text below.

All file shown in main pc and open with excel.

File Home Insert Draw Page Layout Formulas Data Review View Help

Table Design

Tell me what you want to do

Table Name:

Table1

Resize Table

Properties

Summarize with PivotTable

Remove Duplicates

Convert to Range

Tools



Insert Slicer



Export



Refresh



External Table Data

 Header Row Total Row Banded Rows First Column Last Column Banded Columns

Table Style Options

 Filter Button

Quick Styles

Table Styles

Amcache
Entry

A5

Unassociated

	A	B	C	D	E	F	G	H	I	
1	Column16364	ProgramId	FileKeyLastWriteTimestamp	SHA1	IsOsComponent	FullPath	Name	FileExtension	LinkDate	Pro
2	Unassociated	0006a8dc383d	05-07-2023 08:39	32136ffef6	FALSE	c:\users\de	AmcacheF	.exe	24-10-2052 08:04	amc
3	Unassociated	0000f519feec	29-06-2023 08:08	77f2e744c	TRUE	c:\windows	CompatTe	.exe	18-10-2025 04:45	mich
4	Unassociated	0006f3904a4b	29-06-2023 08:09	074349c30	FALSE	c:\program	cookie_ex	.exe	21-06-2023 22:30	mich
5	Unassociated	0000f519feec	29-06-2023 08:01	11eba7b1e	TRUE	c:\windows	csrss.exe	.exe	25-05-1971 13:07	mich
6	Unassociated	0000f519feec	29-06-2023 08:08	0646f8653	TRUE	c:\windows	DeviceCer	.exe	19-05-2039 12:13	mich
7	Unassociated	0006f3904a4b	29-06-2023 08:09	777ac620a	FALSE	c:\program	elevation	.exe	21-06-2023 22:30	mich
8	Unassociated	0006f3904a4b	29-06-2023 08:09	872cc644f	FALSE	c:\program	identity_h	.exe	21-06-2023 22:30	mich
9	Unassociated	0006e0870de2	29-06-2023 08:09	5dedd60f7	FALSE	c:\program	ie_to_edg	.exe	21-06-2023 22:30	ieto
10	Unassociated	0006ae478658	29-06-2023 08:09	690897252	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:16	mich
11	Unassociated	0006868509bc	29-06-2023 08:09	7f6daa619	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:15	mich
12	Unassociated	0006868509bc	29-06-2023 08:09	076f72b14	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:16	mich
13	Unassociated	0006868509bc	29-06-2023 08:09	9f5c3fd02	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:22	mich
14	Unassociated	0006868509bc	29-06-2023 08:09	9f5c3fd02	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:22	mich
15	Unassociated	00060cab34c3	28-06-2023 17:12	3d26b0dc5	FALSE	c:\program	Microsoft	.exe	22-07-2021 01:16	mich
16	Unassociated	0006868509bc	29-06-2023 08:09	b61a5756c	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:16	mich
17	Unassociated	0006868509bc	29-06-2023 08:09	7f7c48ad1	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:16	mich
18	Unassociated	0006868509bc	29-06-2023 08:09	cc92d47f7	FALSE	c:\program	Microsoft	.exe	06-06-2023 18:15	mich
19	Unassociated	000651e5db32	29-06-2023 08:09	7c51ea622	FALSE	c:\program	Microsoft	.exe	21-06-2023 22:30	mich
20	Unassociated	000651e5db32	29-06-2023 08:09	7c51ea622	FALSE	c:\program	Microsoft	.exe	21-06-2023 22:30	mich
21	Unassociated	0000f519feec	29-06-2023 08:04	7e29a8d98	TRUE	c:\windows	MoUseCo	.exe	01-05-2068 18:03	mich
22	Unassociated	0006f3904a4b	29-06-2023 08:09	fea1f23ec	FALSE	c:\program	msedge.e	.exe	21-06-2023 22:30	mich
23	Unassociated	0006707b1ec4	29-06-2023 08:09	92332ecf2	FALSE	c:\program	msedgew	.exe	21-06-2023 22:30	mich

20230706214236_Amcache_Unassoci

Ready Accessibility: Unavailable

Display Settings

100%



Type here to search



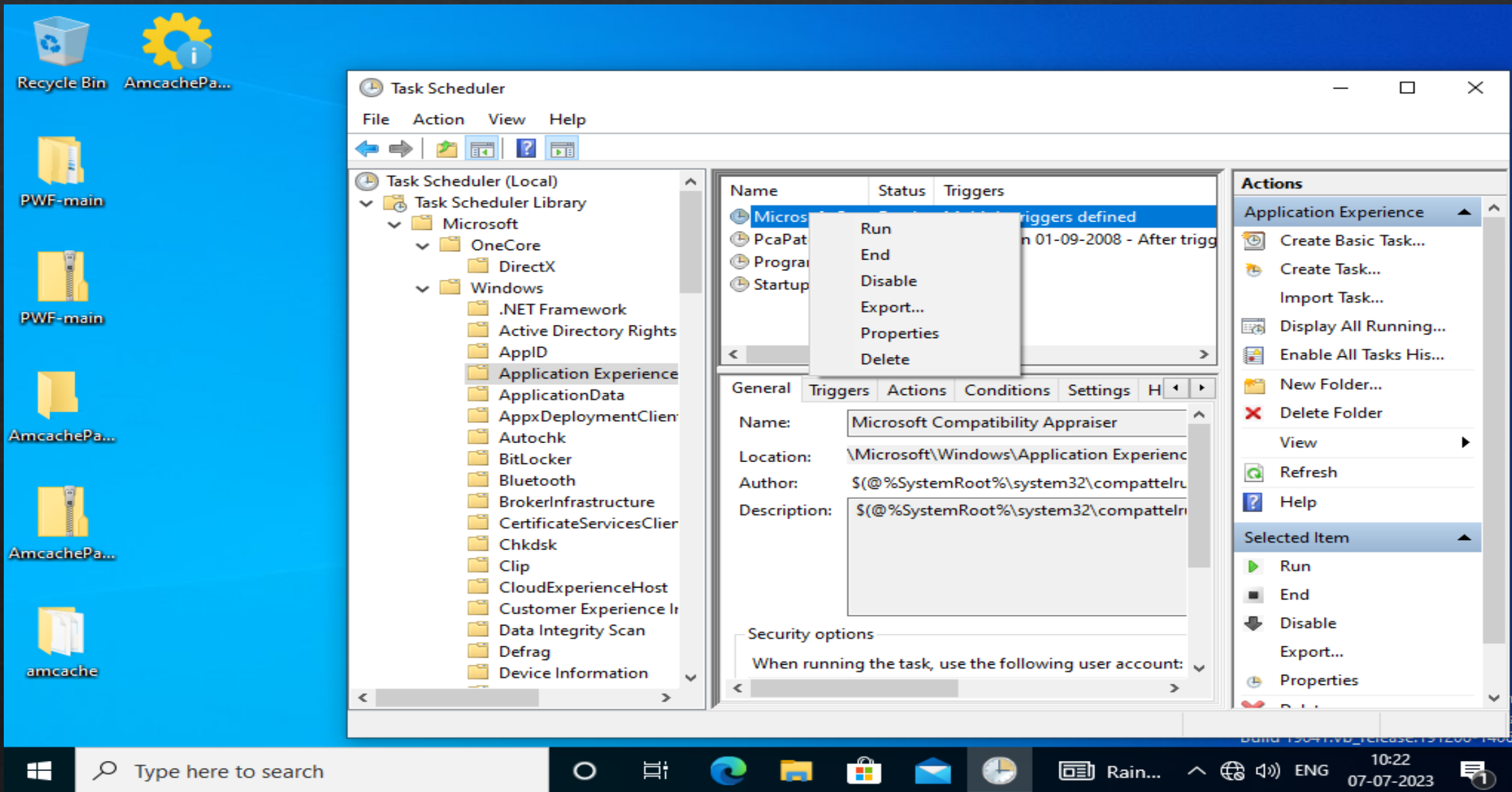
10:29

10-07-2023



2

Open the task Scheduler and click the Application Experience then manually run task.



Administrator: Command Prompt

5 Dir(s) 29,456,506,880 bytes free

```
C:\Users\Denisha\Desktop>AmcacheParser.exe -f C:\Windows\appcompat\Programs\Amcache.hve --csv amcache2
AmcacheParser version 1.5.1.0
```

Author: Eric Zimmerman (saericzimmerman@gmail.com)
<https://github.com/EricZimmerman/AmcacheParser>

Command line: -f C:\Windows\appcompat\Programs\Amcache.hve --csv amcache2

Two transaction logs found. Determining primary log...

Primary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG2, secondary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG1

Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2

Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1

At least one transaction log was applied. Sequence numbers have been updated to 0x0056. New Checksum: 0x28D8E509

'C:\Windows\appcompat\Programs\Amcache.hve' is in use. Rerouting...

Two transaction logs found. Determining primary log...

Primary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG2, secondary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG1

Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2

Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1

At least one transaction log was applied. Sequence numbers have been updated to 0x0056. New Checksum: 0x28D8E509

C:\Windows\appcompat\Programs\Amcache.hve is in new format!

Total file entries found: 145

Total shortcuts found: 50

Total device containers found: 9

Total device PnPs found: 57

Total drive binaries found: 370

Total driver packages found: 2

Found 45 unassociated file entry

Results saved to: amcache2

Total parsing time: 9.353 seconds



Type here to search



28°C



ENG

10:37

10-07-2023



File Explorer window showing the contents of the 'amcache2' folder. The address bar indicates the path: This PC > Downloads > amcache2. The left sidebar shows the navigation pane with 'Downloads' selected. The main pane displays a list of 6 files, all of which are Microsoft Excel spreadsheets (.xlsx) created on 10-07-2023 at 10:37.

Name	Date modified	Type	Size
20230710103733_Amcache_DeviceContai...	10-07-2023 10:37	Microsoft Excel C...	3 KB
20230710103733_Amcache_DevicePnps	10-07-2023 10:37	Microsoft Excel C...	32 KB
20230710103733_Amcache_DriveBinaries	10-07-2023 10:37	Microsoft Excel C...	108 KB
20230710103733_Amcache_DriverPackages	10-07-2023 10:37	Microsoft Excel C...	1 KB
20230710103733_Amcache_ShortCuts	10-07-2023 10:37	Microsoft Excel C...	8 KB
20230710103733_Amcache_Unassociated...	10-07-2023 10:37	Microsoft Excel C...	18 KB

Save the file Amcache2 folder and open with excel.

6 items

Table Name: Table1
 Properties

Summarize with PivotTable
 Remove Duplicates
 Convert to Range
 Tools

Insert Slicer

Export Refresh
 External Table Data

Header Row
 Total Row
 Banded Rows

First Column
 Last Column
 Banded Columns

Table Style Options

Filter Button
 Quick Styles

Output Updated.

E12 FALSE

	A	B	C	D	E	F	G	H	I
1	ApplicationName	ProgramId	FileKeyLastWriteTimestamp	SHA1	IsOsComponent	FullPath	Name	FileExtension	LinkDate
2	Unassociated	0006a8dc383d31dcde22	07-07-2023 04:55	32136ffef	FALSE	c:\users\de AmcacheF.exe			#####
3	Unassociated	0000f519feec486de87e	29-06-2023 08:08	77f2e744c	TRUE	c:\windows CompatTe.exe			#####
4	Unassociated	0006119b97889343334c	10-07-2023 04:53	42d834da:	FALSE	c:\program cookie_ex.exe			#####
5	Unassociated	0000f519feec486de87e	29-06-2023 08:01	11eba7b1c	TRUE	c:\windows csrss.exe	.exe		#####
6	Unassociated	0000f519feec486de87e	29-06-2023 08:08	0646f8653	TRUE	c:\windows DeviceCer.exe			#####
7	Unassociated	0006119b97889343334c	10-07-2023 04:53	3bd5d28ca	FALSE	c:\program elevation.exe			#####
8	Unassociated	0006119b97889343334c	10-07-2023 04:53	cdf846712	FALSE	c:\program identity_t.exe			#####
9	Unassociated	0006137d5eee4dd1f6b	10-07-2023 04:53	d97d5b3d	FALSE	c:\program ie_to_edg.exe			#####
10	Unassociated	00065bf2b4f348de189a	08-07-2023 15:53	6d27b973a	FALSE	c:\program Microsoftl.exe			#####
11	Unassociated	0006aa1f8992cfa6e338k	10-07-2023 04:53	06bac910a	FALSE	c:\program Microsoftl.exe			#####
12	Unassociated	0006aa1f8992cfa6e338k	08-07-2023 15:53	aa15234f0	FALSE	c:\program Microsoftl.exe			#####
13	Unassociated	0006aa1f8992cfa6e338k	08-07-2023 15:53	fed2634cc	FALSE	c:\program Microsoftl.exe			#####
14	Unassociated	0006aa1f8992cfa6e338k	08-07-2023 15:53	ed6642a2c	FALSE	c:\program Microsoftl.exe			#####
15	Unassociated	0006aa1f8992cfa6e338k	08-07-2023 15:53	0c5f3e8a7	FALSE	c:\program Microsoftl.exe			#####
16	Unassociated	00060cab34c3bd2ce1cf	28-06-2023 17:12	3d26b0dc	FALSE	c:\program Microsoftl.exe			#####
17	Unassociated	0006aa1f8992cfa6e338k	08-07-2023 15:53	06bac910a	FALSE	c:\program Microsoftl.exe			#####
18	Unassociated	0006aa1f8992cfa6e338k	08-07-2023 15:53	0a0018108	FALSE	c:\program Microsoftl.exe			#####
19	Unassociated	00060f01fa445416eed8	10-07-2023 04:53	f705161e7	FALSE	c:\program Microsoftl.exe			#####
20	Unassociated	00060f01fa445416eed8	10-07-2023 04:53	f705161e7	FALSE	c:\program Microsoftl.exe			#####
21	Unassociated	0000f519feec486de87e	29-06-2023 08:04	7e29a8d9	TRUE	c:\windows MoUseCo.exe			#####
22	Unassociated	0006e71e182965d4146f	10-07-2023 04:53	f92f04998	FALSE	c:\program MpCopyA.exe			#####
23	Unassociated	0006dc1a176320b5dbb	10-07-2023 04:53	45d7b8e9	FALSE	c:\windows MoSigStu.exe			#####

20230710103733_Amcache_Unassoci

4. Windows Prefetch Analysis

Accessing Prefetch Files for Forensic Analysis. A digital forensic investigation often aims to determine the activities of a user on a computer. Prefetch files are an important type of evidence, which provide detailed information about the programs that were run on a computer.

In the windows 10 target system many prefetch files available in this path.

File Explorer window titled "prefetch" showing the directory "C:\Cases\F\Windows\prefetch". The window displays a list of 180 prefetch files. The left sidebar shows "Quick access" and "This PC" sections. The main pane displays a list of files with columns for Name, Date modified, Type, and Size.

Name	Date modified	Type	Size
AM_BASE.EXE-808FC880.pf	29-06-2023 08:06	PF File	2 KB
AM_DELTA.EXE-B7261F63.pf	29-06-2023 08:07	PF File	2 KB
AM_ENGINE.EXE-69ACF71F.pf	29-06-2023 08:06	PF File	3 KB
APPLICATIONFRAMEHOST.EXE-CCEEF75...	29-06-2023 08:05	PF File	15 KB
AUDIODG.EXE-BDFD3029.pf	29-06-2023 08:03	PF File	6 KB
BACKGROUNDTASKHOST.EXE-145A3777.pf	28-06-2023 16:21	PF File	12 KB
BACKGROUNDTASKHOST.EXE-A89D33B8...	29-06-2023 08:02	PF File	14 KB
BACKGROUNDTRANSFERHOST.EXE-4FEE...	28-06-2023 16:24	PF File	14 KB
BACKGROUNDTRANSFERHOST.EXE-298E...	28-06-2023 16:46	PF File	8 KB
BACKGROUNDTRANSFERHOST.EXE-CF5...	28-06-2023 16:52	PF File	10 KB
BYTECODEGENERATOR.EXE-C1E9BCE6.pf	29-06-2023 08:25	PF File	8 KB
CLOUDEXPERIENCEHOSTBROKER.EXE-E8...	28-06-2023 16:19	PF File	14 KB
CMD.EXE-4A81B364.pf	28-06-2023 16:32	PF File	1 KB
COMPATTELRUNNER.EXE-DB97728F.pf	28-06-2023 17:13	PF File	3 KB
CONHOST.EXE-1F3E9D7E.pf	29-06-2023 08:25	PF File	10 KB
CONSENT.EXE-531BD9EA.pf	29-06-2023 08:03	PF File	25 KB
CSC.EXE-67679278.pf	28-06-2023 16:42	PF File	9 KB
CSRSS.EXE-3FE41F7E.pf	28-06-2023 16:20	PF File	5 KB
CVTRES.EXE-F2B7602E.pf	28-06-2023 16:42	PF File	3 KB
DLLHOST.EXE-5E46FA0D.pf	29-06-2023 08:14	PF File	4 KB
DLLHOST.EXE-28A8211F.pf	29-06-2023 08:13	PF File	12 KB
DLLHOST.EXE-61F58501.pf	28-06-2023 16:19	PF File	8 KB
DLLHOST.EXE-504C779A.pf	29-06-2023 08:11	PF File	5 KB

180 items

Open the PECmd tool and type the command for particular application.

The screenshot shows a Windows File Explorer window titled "Get-ZimmermanTools" with the address bar set to "C:\Tools\Get-ZimmermanTools". The left sidebar shows the navigation pane with "This PC" and "SDT_x64FREE_EN" expanded. The main pane displays a list of files and folders. The file "PECmd" is selected and highlighted in grey.

Name	Date modified	Type	Size
EvtxECmd	28-06-2023 13:40	File folder	
EZViewer	28-06-2023 13:40	File folder	
Hasher	28-06-2023 13:41	File folder	
iisGeolocate	28-06-2023 13:44	File folder	
JumpListExplorer	28-06-2023 13:41	File folder	
MFTExplorer	28-06-2023 13:41	File folder	
RECcmd	28-06-2023 13:41	File folder	
RegistryExplorer	28-06-2023 13:42	File folder	
SDBExplorer	28-06-2023 13:42	File folder	
ShellBagsExplorer	01-07-2023 10:36	File folder	
SQLLECmd	28-06-2023 13:43	File folder	
TimelineExplorer	01-07-2023 05:43	File folder	
XWFIM	28-06-2023 13:44	File folder	
!!!RemoteFileDetails	28-06-2023 13:44	CSV File	5 KB
AmcacheParser	21-05-2023 11:49	Application	4,661 KB
AppCompatCacheParser	07-03-2023 15:13	Application	4,523 KB
bstrings	20-05-2022 12:38	Application	3,997 KB
ChangeLog	28-06-2023 13:44	Text Document	33 KB
Get-ZimmermanTools	18-05-2023 14:24	Windows PowerS...	24 KB
JLECmd	13-03-2023 17:06	Application	4,792 KB
LECmd	04-03-2023 10:30	Application	5,063 KB
MFTECmd	20-10-2022 13:37	Application	4,409 KB
PECmd	28-01-2022 12:08	Application	3,885 KB

32 items | 1 item selected 3.79 MB

05:07
16-07-2023

Administrator: C:\Windows\System32\cmd.exe

Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Tools\Get-ZimmermanTools>PECmd.exe

Description:

PECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)

<https://github.com/EricZimmerman/PECmd>

Examples: PECmd.exe -f "C:\Temp\CALC.EXE-3FBEB7FD.pf"
PECmd.exe -f "C:\Temp\CALC.EXE-3FBEB7FD.pf" --json "D:\jsonOutput" --jsonpretty
PECmd.exe -d "C:\Temp" -k "system32, fonts"
PECmd.exe -d "C:\Temp" --csv "c:\temp" --csvf foo.csv --json c:\temp\json
PECmd.exe -d "C:\Windows\Prefetch"

Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes

Usage:

PECmd [options]

Options:

-f <f> File to process. Either this or -d is required
-d <d> Directory to recursively process. Either this or -f is required
-k <k> Comma separated list of keywords to highlight in output. By default, 'temp' and 'tmp' are highlighted. Any additional keywords will be added to these
-o <o> When specified, save prefetch file bytes to the given path. Useful to look at decompressed Win10 files
-q Do not dump full details about each file processed. Speeds up processing when using --json or --csv [default: False]
--json <json> Directory to save JSON formatted results to. Be sure to include the full path in double quotes
--jsonf <jsonf> File name to save JSON formatted results to. When present, overrides default name
--csv <csv> Directory to save CSV formatted results to. Be sure to include the full path in double quotes
--csvf <csvf> File name to save CSV formatted results to. When present, overrides default name
--html <html> Directory to save xhtml formatted results to. Be sure to include the full path in double quotes
--dt <dt> The custom date/time format to use when displaying time stamps. See <https://goo.gl/CNVq0k> for options [default: yyyy-MM-dd HH:mm:ss]



06:08

07-07-2023



Administrator: C:\Windows\System32\cmd.exe

Either -f or -d is required. Exiting

C:\Tools\Get-ZimmermanTools>PECmd.exe -f C:\Cases\F\Windows\prefetch\APPLICATIONFRAMEHOST.EXE-CCEEF759.pf
PECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
<https://github.com/EricZimmerman/PECmd>

Command line: -f C:\Cases\F\Windows\prefetch\APPLICATIONFRAMEHOST.EXE-CCEEF759.pf

Keywords: temp, tmp

Processing C:\Cases\F\Windows\prefetch\APPLICATIONFRAMEHOST.EXE-CCEEF759.pf

Created on: 2023-06-28 16:24:19
Modified on: 2023-06-29 08:05:09
Last accessed on: 2023-06-29 08:05:09

Executable name: APPLICATIONFRAMEHOST.EXE
Hash: CCEEF759
File size (bytes): 63,002
Version: Windows 10 or Windows 11

Run count: 3
Last run: 2023-06-29 08:04:59
Other run times: 2023-06-28 16:35:05, 2023-06-28 16:24:09

Volume information:

#0: Name: \VOLUME{01d9aa46f526b4aa-4af59951} Serial: 4AF59951 Created: 2023-06-29 05:02:52 Directories: 20 File references: 106

Directories referenced: 20

00: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES
01: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS
02: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_NEUTRAL_SPLIT.SC



06:10

07-07-2023



06

Directories referenced: 20

```
00: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES
01: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS
02: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_NEUTRAL_SPLIT.SCALE-100_8WEKYB3D8BBWE
03: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_NEUTRAL_SPLIT.SCALE-100_8WEKYB3D8BBWE\IMAGES
04: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_X64__8WEKYB3D8BBWE
05: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_X64__8WEKYB3D8BBWE\MICROSOFT.SYSTEM.PACKAGE.METADATA
06: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSSTORE_11910.1002.5.0_NEUTRAL_SPLIT.SCALE-100_8WEKYB3D8BBWE
07: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSSTORE_11910.1002.5.0_NEUTRAL_SPLIT.SCALE-100_8WEKYB3D8BBWE\ASSETS
08: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSSTORE_11910.1002.5.0_NEUTRAL_SPLIT.SCALE-100_8WEKYB3D8BBWE\ASSETS\APPTILES
09: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS
10: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\FONTS
11: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\GLOBALIZATION
12: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\GLOBALIZATION\SORTING
13: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\IMMERSIVECONTROL PANEL
14: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\IMMERSIVECONTROL PANEL\IMAGES
15: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\RESCACHE
16: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\RESCACHE\_MERGED
17: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\RESCACHE\_MERGED\987641329
18: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32
19: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\EN-US
```

Files referenced: 80

```
00: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\APPLICATIONFRAMEHOST.EXE (Executable: True)
02: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\KERNEL32.DLL
```



06:11

07-07-2023



5. Windows Prefetch Timeline Analysis

In this command all prefetch file store in specific folder and open with timeline explorer

```
Administrator: C:\Windows\System32\cmd.exe
197: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\MSVCP110_WIN.DLL
198: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\WINDOWS.SYSTEM.DIAGNOSTICS.DLL
199: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\WINMETADATA\WINDOWS.UI.WINMD
200: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\WINMETADATA\WINDOWS.SECURITY.WINMD
201: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\WINDOWS.SECURITY.AUTHENTICATION.WEB.CORE.DLL
202: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\ONECORECOMMONPROXYSTUB.DLL
203: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\EN-US\WINDOWS.SECURITY.AUTHENTICATION.WEB.CORE.DLL.MUI
204: \VOLUME{01d9aa46f526b4aa-4af59951}\USERS\DENISHA\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTOFFICEHUB_8WEKYB3D8BBWE\AC\IN
ETCACHE\MSIMGSIZ.DAT
205: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\WINDOWSCODECS.DLL
206: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_X64__8WEKYB3D8B
BWE\MYOFFICE.RUNTIMECOMPONENTS.WINMD
207: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_X64__8WEKYB3D8B
BWE\MYOFFICE.RUNTIMECOMPONENTS.DLL
208: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.VCLIBS.140.00_14.0.27323.0_X64__8WEKYB3D8BBWE\MSV
CP140_APP.DLL
209: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.VCLIBS.140.00_14.0.27323.0_X64__8WEKYB3D8BBWE\VCR
UNTIME140_APP.DLL
210: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\WEBPLATSTORAGESERVER.DLL
211: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\LOGONCLI.DLL
212: \VOLUME{01d9aa46f526b4aa-4af59951}\USERS\DENISHA\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTOFFICEHUB_8WEKYB3D8BBWE\AC\IN
ETCACHE\S3F01B3R\HERO-IMAGE-DESKTOP-F6720A4145[1].JPG
213: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\EN-US\WINDOWS.STORAGE.DLL.MUI
214: \VOLUME{01d9aa46f526b4aa-4af59951}\USERS\DENISHA\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTOFFICEHUB_8WEKYB3D8BBWE\AC\IN
ETCACHE\S3F01B3R\THIRDPARTYNOTICE[1].HTM
215: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\CRYPTOWINRT.DLL
216: \VOLUME{01d9aa46f526b4aa-4af59951}\USERS\DENISHA\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTOFFICEHUB_8WEKYB3D8BBWE\LOCAL
STATE\THIRDPARTYNOTICE.HTML.~TMP (Keyword: True)

----- Processed C:\Cases\F\Windows\prefetch\WWAHOST.EXE-DB0D8801.pf in 0.86211480 seconds -----
Processed 180 out of 180 files in 76.5676 seconds

CSV output will be saved to C:\Cases\Analysis\Execution\20230716051531_PECmd_Output.csv
CSV time line output will be saved to C:\Cases\Analysis\Execution\20230716051531_PECmd_Output_Timeline.csv

C:\Tools\Get-ZimmermanTools>PECmd.exe -d C:\Cases\F\Windows\prefetch --csv C:\Cases\Analysis\Execution\
```



Execution

File Home Share View

← → ↕ ↑ This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > Analysis > Execution Search Execution

Name	Date modified	Type	Size
20230705061123_Windows10C_11_SYSTE...	05-07-2023 06:11	CSV File	45 KB
20230705080017_Amcache_DeviceContai...	05-07-2023 08:00	CSV File	3 KB
20230705080017_Amcache_DevicePnps	05-07-2023 08:00	CSV File	27 KB
20230705080017_Amcache_DriveBinaries	05-07-2023 08:00	CSV File	107 KB
20230705080017_Amcache_DriverPackages	05-07-2023 08:00	CSV File	1 KB
20230705080017_Amcache_ShortCuts	05-07-2023 08:00	CSV File	8 KB
20230705080017_Amcache_Unassociated...	05-07-2023 08:00	CSV File	13 KB
20230707061607_PECmd_Output	07-07-2023 06:16	CSV File	1,374 KB
20230707061607_PECmd_Output_Timeline	07-07-2023 06:16	CSV File	54 KB
20230716051531_PECmd_Output	16-07-2023 05:15	CSV File	1,374 KB
20230716051531_PECmd_Output_Timeline	16-07-2023 05:15	CSV File	54 KB

Quick access: Desktop, Downloads, Documents, Pictures, Evidence, Execution, NTFS, Registry

This PC: 3D Objects, Desktop, Documents, Downloads, Music, Pictures, Videos, SDT_x64FREE_EN, CD Drive (D:) Vir, Downloads (\\V)

11 items | 1 item selected 1.34 MB

Open this file in timeline explorer

Show the All prefetch file with time

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

20230716051531_PECmd_Output.csv

Drag a column header here to group by that column Find

	ote	Source Filename	Volume1Seri...	Source Created	Source Modif...	Source A
Y	lc	RBc	RBc	=	=	=
▶		C:\Cases\F\Windows\prefetch\AM_BASE.EXE-808FC88...		2023-06-29 08:06:55	2023-06-29 0...	2023-06-
		C:\Cases\F\Windows\prefetch\AM_DELTA.EXE-B7261F...		2023-06-29 08:07:23	2023-06-29 0...	2023-06-
		C:\Cases\F\Windows\prefetch\AM_ENGINE.EXE-69ACF...		2023-06-29 08:06:22	2023-06-29 0...	2023-06-
		C:\Cases\F\Windows\prefetch\APPLICATIONFRAMEHOS...		2023-06-28 16:24:19	2023-06-29 0...	2023-06-
		C:\Cases\F\Windows\prefetch\AUDIODG.EXE-BDFD302...		2023-06-28 16:14:35	2023-06-29 0...	2023-06-
		C:\Cases\F\Windows\prefetch\BACKGROUNDTASKHOST....		2023-06-28 16:20:20	2023-06-28 1...	2023-06-
		C:\Cases\F\Windows\prefetch\BACKGROUNDTASKHOST....		2023-06-28 16:21:51	2023-06-29 0...	2023-06-
		C:\Cases\F\Windows\prefetch\BACKGROUNDTRANSFERH...		2023-06-28 16:46:00	2023-06-28 1...	2023-06-
		C:\Cases\F\Windows\prefetch\BACKGROUNDTRANSFERH...		2023-06-28 16:24:21	2023-06-28 1...	2023-06-
		C:\Cases\F\Windows\prefetch\BACKGROUNDTRANSFERH...		2023-06-28 16:52:04	2023-06-28 1...	2023-06-
		C:\Cases\F\Windows\prefetch\BYTECODEGENERATOR.E...		2023-06-28 16:10:07	2023-06-29 0...	2023-06-
		C:\Cases\F\Windows\prefetch\CLOUDEXPERIENCEHOST...		2023-06-28 16:14:15	2023-06-28 1...	2023-06-
		C:\Cases\F\Windows\prefetch\CMD.EXE-4A81B364.pf		2023-06-28 16:32:49	2023-06-28 1...	2023-06-
		C:\Cases\F\Windows\prefetch\COMPATTELRUNNER.EXE...		2023-06-28 17:13:24	2023-06-28 1...	2023-06-
		C:\Cases\F\Windows\prefetch\CONHOST.EXE-1F3E9D7...		2023-06-28 16:13:22	2023-06-29 0...	2023-06-
		C:\Cases\F\Windows\prefetch\CONSENT.EXE-531BD9E...		2023-06-28 16:20:43	2023-06-29 0...	2023-06-
		C:\Cases\F\Windows\prefetch\CSC.EXE-67679278.pf		2023-06-28 16:42:40	2023-06-28 1...	2023-06-
		C:\Cases\F\Windows\prefetch\CSRSS.EXE-3FE41F7E....		2023-06-28 16:20:38	2023-06-28 1...	2023-06-
		C:\Cases\F\Windows\prefetch\CVTRES.EXE-F2B7602E...		2023-06-28 16:42:40	2023-06-28 1...	2023-06-

Auto run keys Analysis

Autorun and run keys are registry entries that allow programs to execute automatically when a device is connected or a user logs on. Malicious actors can use them to launch malware, bypass security controls, and maintain persistence on compromised hosts.

Registry Explorer v1.6.0.0
File Tools Options Bookmarks (29/0) View Help

Registry hives (2) Available bookmarks (59/0)

run Find

Key name

- C:\Cases\Analysis\Registry\NTUSER.DAT
 - CurrentVersion
 - Run
 - RunMRU
 - RunOnce
 - Shell
- C:\Cases\Analysis\Registry\SOFTWARE
 - Channels

Bookmark information

Hive: C:\Cases\Analysis\Registry\SOFTWARE
Category: Autoruns
Name: Run
Key path: Microsoft\Windows\CurrentVersion\Run
Short description: Run key
Long description: Used to automatically start programs

Values

Drag a column header here to group by that column

	Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
▼	REG	REG	REG	REG	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
▶	SecurityHealth	RegExpandSz	%windir%\syste...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
	VBoxTray	RegExpandSz	%SystemRoot%...	00-00-1D-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>

You can insert the NTUSER hives in Registry Explorer and then search run.

Type viewer Slack viewer Binary viewer

Value name: SecurityHealth
Value type: RegExpandSz

Key: Microsoft\Windows\CurrentVersion\Run Value: SecurityHealth Collapse all hives

Selected hive: NTUSER.DAT Last write: 29-06-2023 08:01:53 +00:00 2 of 2 values shown (100.00%) Hidden keys: 0 1

Registry hives (2) Available bookmarks (59/0)

run | Find

Key name

- C:\Cases\Analysis\Registry\NTUSER.DAT
- C:\Cases\Analysis\Registry\SOFTWARE
 - Channels
 - CurrentVersion
 - CurrentVersion
 - Image File Execution Options
 - Internet Explorer
 - Run

Bookmark information

Hive: C:\Cases\Analysis\Registry\SOFTWARE

Category: Autoruns

Name: Run

Key path: Microsoft\Windows\CurrentVersion\Run

Short description: Run key

Long description: Used to automatically start programs

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
RC	RC	RC	RC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SecurityHealth	RegExpandSz	%windir%\syste...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
VBoxTray	RegExpandSz	%SystemRoot%...	00-00-1D-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>

You can insert the Software hive in Registry Explorer and search run and show the autorun activities.

Type viewer Slack viewer Binary viewer

Value name: SecurityHealth

Value type: RegExpandSz

Registry

File Home Share View

This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > Analysis > Registry

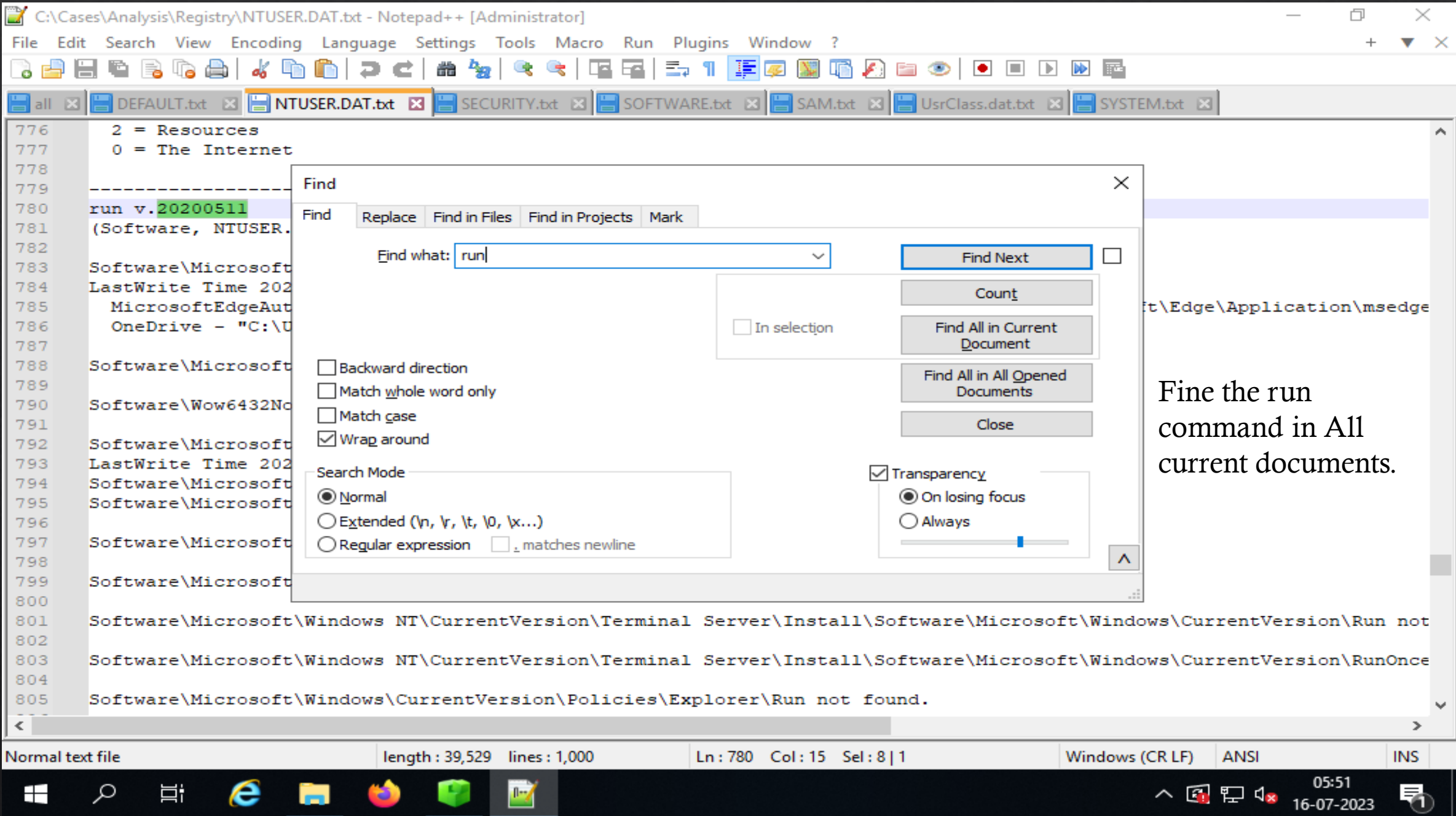
Search Registry

Name	Date modified	Type	Size
UsrClass.dat	01-07-2023 10:55	Text Document	15 KB
UsrClass.dat	29-06-2023 09:07	DAT File	3,328 KB
SYSTEM	01-07-2023 10:55	Text Document	373 KB
SYSTEM	29-06-2023 09:08	File	11,008 KB
SOFTWARE	01-07-2023 10:55	Text Document	2,476 KB
SOFTWARE	29-06-2023 09:08	File	68,608 KB
SECURITY	01-07-2023 10:55	Text Document	4 KB
SECURITY	29-06-2023 09:08	File	32 KB
SAM	01-07-2023 10:55	Text Document	8 KB
SAM	29-06-2023 09:08	File	64 KB
NTUSER.DAT	01-07-2023 10:02	Text Document	39 KB
NTUSER.DAT	29-06-2023 09:07	DAT File	1,024 KB
DEFAULT	01-07-2023 10:55	Text Document	16 KB
DEFAULT	29-06-2023 09:08	File	512 KB

Open
Print
Edit
Edit with Notepad++
Share
Open with >
Restore previous versions
Send to >
Cut
Copy
Create shortcut
Delete
Rename
Properties

NTUSER hives open with Notepad++.

14 items | 1 item selected 38.6 KB



Fine the run command in All current documents.

C:\Cases\Analysis\Registry\NTUSER.DAT.txt - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

all x DEFAULT.txt x NTUSER.DAT.txt x SECURITY.txt x SOFTWARE.txt x SAM.txt x UsrClass.dat.txt x SYSTEM.txt x

```
776 2 = Resources
777 0 = The Internet
778
779 -----
780 run v.20200511
781 (Software, NTUSER.DAT) [Autostart] Get autostart key contents from Software hive
782
783 Software\Microsoft\Windows\CurrentVersion\Run
784 LastWrite Time 2023-06-28 17:52:55Z
785 MicrosoftEdgeAutoLaunch_1ED6AFCC191394652DA0C4ECFC733304 - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge
786 OneDrive - "C:\Users\Denisha\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
787
788 Software\Microsoft\Windows\CurrentVersion\Run has no subkeys.
789
790 Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.
791
792 Software\Microsoft\Windows\CurrentVersion\RunOnce
793 LastWrite Time 2023-06-28 16:32:46Z
794 Software\Microsoft\Windows\CurrentVersion\RunOnce has no values.
```

Search results - (25 hits)

Search "run" (25 hits in 1 file of 1 searched)

C:\Cases\Analysis\Registry\NTUSER.DAT.txt (25 hits)

```
Line 465: (NTUSER.DAT) Autostart - get Command Processor\AutoRun value from NTUSER.DAT hive
Line 564: (NTUSER.DAT) Gets load and run values from user hive
Line 571: run value not found.
Line 780: run v.20200511
Line 783: Software\Microsoft\Windows\CurrentVersion\Run
Line 788: Software\Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 790: Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.
Line 792: Software\Microsoft\Windows\CurrentVersion\RunOnce
```

Normal text file length: 39,529 lines: 1,000 Ln: 783 Col: 46 Sel: 3 | 1 Windows (CR LF) ANSI INS

05:51 16-07-2023

```
C:\Cases\Analysis\Registry\SOFTWARE.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
all x DEFAULT.txt x NTUSER.DAT.txt x SECURITY.txt x SOFTWARE.txt x SAM.txt x UsrClass.dat.txt x SYSTEM.txt x
40290 Software\Policies\Microsoft\Windows\PowerShell not found.
40291 Policies\Microsoft\Windows\PowerShell not found.
40292 -----
40293 -----
40294 run v.20200511
40295 (Software, NTUSER.DAT) [Autostart] Get autostart key contents from Software hive
40296
40297 Microsoft\Windows\CurrentVersion\Run
40298 LastWrite Time 2023-06-29 08:01:53Z
40299     VBoxTray - %SystemRoot%\system32\VBoxTray.exe
40300     SecurityHealth - %windir%\system32\SecurityHealthSystray.exe
40301
40302 Microsoft\Windows\CurrentVersion\Run has no subkeys.
40303
40304 Microsoft\Windows\CurrentVersion\RunOnce
40305 LastWrite Time 2019-12-07 09:17:27Z
40306 Microsoft\Windows\CurrentVersion\RunOnce has no values.
40307 Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
40308
40309 Microsoft\Windows\CurrentVersion\RunServices not found.
40310
40311 Wow6432Node\Microsoft\Windows\CurrentVersion\Run
40312 LastWrite Time 2019-12-07 09:17:27Z
40313 Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no values.
40314 Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no subkeys.
40315
40316 Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
40317 LastWrite Time 2019-12-07 09:17:27Z
40318 Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no values.
40319 Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
-----
Normal text file      length : 25,34,532  lines : 41,650      Ln : 40,297  Col : 1  Sel : 36 | 1      Windows (CR LF)  UTF-8  INS
Windows taskbar: 05:52 16-07-2023
```

Find the run command in software hives in current all documents.

Startup Folder Analysis

Two location mention for startup folder.

1. C:\Cases\F\ProgramData\Microsoft\Windows\Start Menu
2. C:\Cases\F\Users\Denisha\AppData\Roaming\Microsoft\Windows

Open the given file location with ubuntu linux and use mnt directory , show mnt.csv file and using grep command show startup folders and scripts.

```
Select forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/NTFS
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases$ cd ../../..
forensic@WIN-AJDB7GOIQEJ:/$ cd /mnt/c/Cases/Analysis/NTFS
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/NTFS$ ls -l
total 58904
-rwxrwxrwx 1 forensic forensic 60316000 Jul  1 16:42 MFT.csv
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/NTFS$ grep startup MFT.csv
14800,1,True,5280,1,.\Windows\WinSxS,amd64_microsoft-windows-s_32_kf_comm_startup_31bf3856ad364e35_10.0.19041.1_none_b2014b56ea660ec9,,0,1,,True,False,False,True,False,False,None,Windows,2019-12-07 09:09:10.0828868,2023-06-29 05:03:11.0746274,2019-12-07 09:09:10.0828868,2023-06-29 05:03:11.0746274,2023-06-29 05:32:49.9658981,2023-06-29 05:03:11.0746274,2019-12-07 09:09:10.0828868,2023-06-29 05:03:11.0746274,0,185351776,551,,DSC,
14985,1,True,5280,1,.\Windows\WinSxS,amd64_microsoft-windows-s..estartup-change-pin_31bf3856ad364e35_10.0.19041.1237_none_665f7346099d6350,,0,1,,True,False,False,True,False,False,None,Windows,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,2023-06-29 05:32:50.0439843,2023-06-29 05:03:11.2621355,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,0,185379446,551,,DSC,
14986,1,True,14985,1,.\Windows\WinSxS\amd64_microsoft-windows-s..estartup-change-pin_31bf3856ad364e35_10.0.19041.1237_none_665f7346099d6350,f,,0,1,,True,False,False,True,False,False,None,DosWindows,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,2023-06-29 05:32:50.0439843,2023-06-29 05:03:11.2621355,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,0,185379176,551,,DSC,
14987,1,True,14985,1,.\Windows\WinSxS\amd64_microsoft-windows-s..estartup-change-pin_31bf3856ad364e35_10.0.19041.1237_none_665f7346099d6350,r,,0,1,,True,False,False,True,False,False,None,DosWindows,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,2023-06-29 05:32:50.0439843,2023-06-29 05:03:11.2621355,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,0,185379310,551,,DSC,
15238,1,True,5280,1,.\Windows\WinSxS,amd64_microsoft-windows-s..ngshandlers-startup_31bf3856ad364e35_10.0.19041.746_none_522701f930d0ca36,,0,1,,True,False,False,True,False,False,None,Windows,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,2023-06-29 05:32:50.1371573,2023-06-29 05:03:11.4972405,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,0,185417952,551,,DSC,
15239,1,True,15238,1,.\Windows\WinSxS\amd64_microsoft-windows-s..ngshandlers-startup_31bf3856ad364e35_10.0.19041.746_none_522701f930d0ca36,f,,0,1,,True,False,False,True,False,False,None,DosWindows,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,2023-06-29 05:32:50.1371573,2023-06-29 05:03:11.4972405,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,0,185417687,551,,DSC,
15240,1,True,15238,1,.\Windows\WinSxS\amd64_microsoft-windows-s..ngshandlers-startup_31bf3856ad364e35_10.0.19041.746_none_522701f930d0ca36,r,,0,1,,True,False,False,True,False,False,None,DosWindows,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,2023-06-29 05:32:50.1371573,2023-06-29 05:03:11.4972405,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,0,185417829,551,,DSC,
15365,1,True,5280,1,.\Windows\WinSxS,amd64_microsoft-windows-s..restartup-baaupdate_31bf3856ad364e35_10.0.19041.1_none_ec3fd410728598b3,,0,1,,True,False,False,True,False,False,None,Windows,2019-12-07 09:10:43.7738833,2023-06-29 05:03:11.6235335,2019-12-07 09:51:57.4131230,2023-06-29 05:03:11.6235335,2023-06-29 05:32:50.1684200,2023-06-29 05:03:11.6235335,2019-12-07 09:51:57.4131230,2023-06-29 05:03:11.6235335,0,185417829,551,,DSC,
```

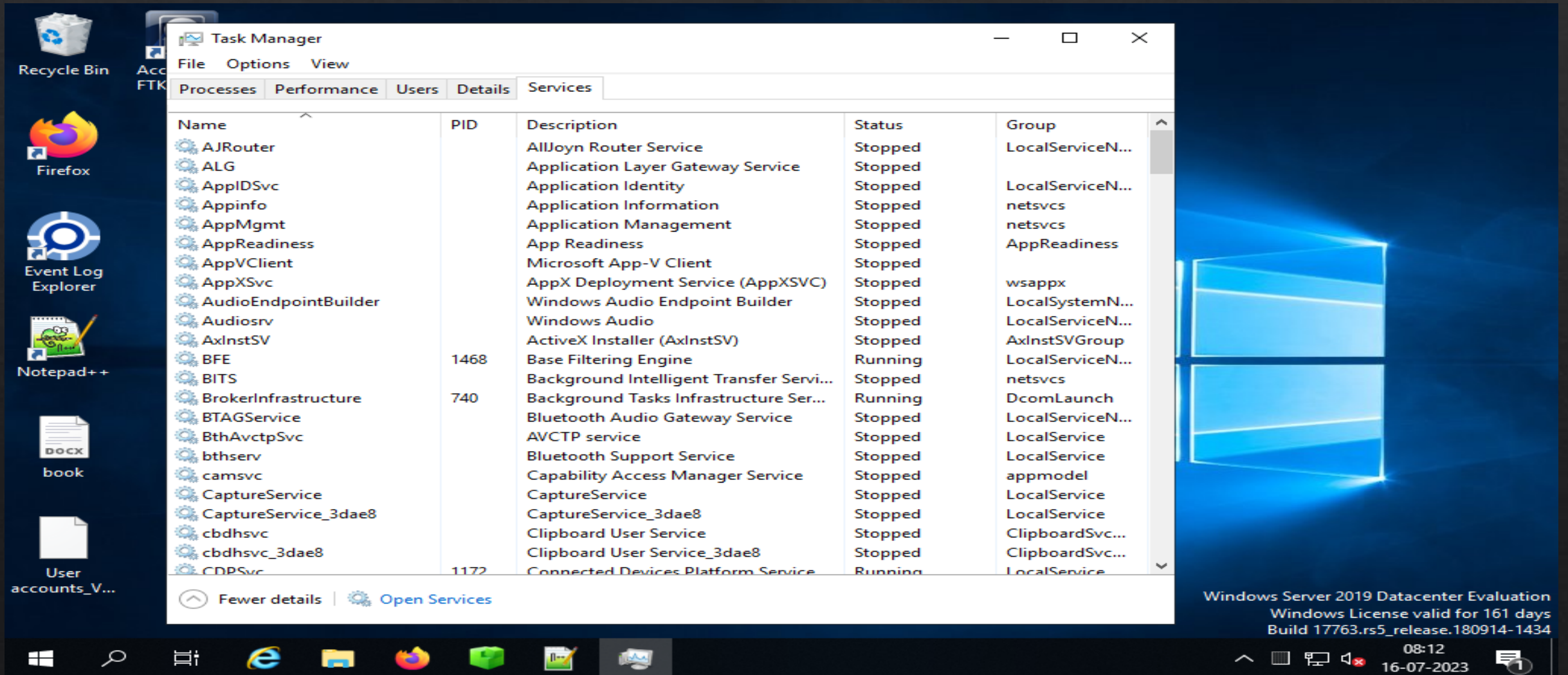


```
Select forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/NTFS
06-29 05:31:49.2620434,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.2620434,2023-06-29 05:31:49.2620434,,2021-10-06 13:54:
19.8017226,2023-06-29 05:31:49.2620434,0,174624611,587,,,$DSC,
95546,1,True,24202,1,.\Windows\WinSxS\wow64_microsoft-windows-securestartup-core_31bf3856ad364e35_10.0.19041.1237_none_b3f20c
1adbb3de92\r,fveapibase.dll,.dll,9395,1,,False,False,False,True,False,False,Archive,Windows,2021-10-06 13:54:19.8017226,2023-
06-29 05:31:49.2620434,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.2620434,2023-06-29 05:31:49.2620434,,2021-10-06 13:54:
19.8017226,2023-06-29 05:31:49.2620434,0,174624639,587,,,$DSC,
95547,1,True,24201,1,.\Windows\WinSxS\wow64_microsoft-windows-securestartup-core_31bf3856ad364e35_10.0.19041.1237_none_b3f20c
1adbb3de92\f,fveapibase.dll,.dll,16379,1,,False,False,False,True,False,False,Archive,Windows,2021-10-06 13:54:19.7861032,2023
-06-29 05:31:49.2620434,2021-10-06 13:54:19.7861032,2023-06-29 05:31:49.2620434,2023-06-29 05:31:49.2620434,,2021-10-06 13:54
:19.7861032,2023-06-29 05:31:49.2620434,0,174624723,587,,,$DSC,
95550,1,True,24202,1,.\Windows\WinSxS\wow64_microsoft-windows-securestartup-core_31bf3856ad364e35_10.0.19041.1237_none_b3f20c
1adbb3de92\r,fveapi.dll,.dll,28304,1,,False,False,False,True,False,False,Archive,DosWindows,2021-10-06 13:54:19.8017226,2023-
06-29 05:31:49.3104659,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.3104659,2023-06-29 05:31:49.3104659,,2021-10-06 13:54:
19.8017226,2023-06-29 05:31:49.3104659,0,174624787,587,,,$DSC,
105628,9,True,105627,9,.\AtomicRedTeam\atomics\T1547.001\src,batstartup.bat,.bat,34,1,,False,False,False,False,True,True,Arch
ive,Windows,2023-06-28 17:57:10.9778236,,2022-04-27 12:44:48.0000000,2023-06-28 17:57:10.9778236,2023-06-28 17:57:10.9911164,
2023-06-28 17:57:10.9778236,2023-06-28 17:57:10.9778236,,17383848,374819591,2307,,,
105629,9,True,105627,9,.\AtomicRedTeam\atomics\T1547.001\src,jsestartup.jse,.jse,44,1,,False,False,False,False,True,True,Arch
ive,Windows,2023-06-28 17:57:10.9911164,,2022-04-27 12:44:48.0000000,2023-06-28 17:57:10.9911164,2023-06-28 17:57:10.9911164,
,2023-06-28 17:57:10.9911164,,17384288,374820360,2307,,,
105630,9,True,105627,9,.\AtomicRedTeam\atomics\T1547.001\src,vbsstartup.vbs,.vbs,44,1,,False,False,False,False,True,True,Arch
ive,Windows,2023-06-28 17:57:10.9911164,,2022-04-27 12:44:48.0000000,2023-06-28 17:57:10.9911164,2023-06-28 17:57:10.9911164,
,2023-06-28 17:57:10.9911164,,17384728,374821123,2307,,,
30028,2,False,601,1,.\PathUnknown\Directory with ID 0x00000259-00000001,startup_background.png,.png,175574,1,,False,False,Fal
se,True,False,False,Archive|RecallOnOpen,Windows,2019-12-07 09:52:31.7251271,2023-06-29 05:04:24.6937921,2019-12-07 09:52:31.
7251271,2023-06-29 05:04:24.6937921,2023-06-28 16:07:58.5868695,2023-06-29 05:04:24.6937921,2023-06-28 16:07:58.5700946,2023-
06-29 05:04:24.6937921,2333896,437919618,1266,,,
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/NTFS$ _
```

Show the bat script in target system

Windows Services

A Windows service is an application that usually serves a core operating system function running in the background and has no user interface.



The screenshot displays the Windows Task Manager application with the 'Services' tab selected. The window title is 'Task Manager' and it includes a menu bar with 'File', 'Options', and 'View'. Below the menu bar are tabs for 'Processes', 'Performance', 'Users', 'Details', and 'Services'. The 'Services' tab is active, showing a table of system services. The table has columns for Name, PID, Description, Status, and Group. The services listed include various system components like routers, gateways, application identity, and background tasks infrastructure. The status of each service is indicated as either 'Running' or 'Stopped'. The background shows a Windows desktop with icons for Recycle Bin, Firefox, Event Log Explorer, Notepad++, and User accounts. The taskbar at the bottom shows the Start button, search icon, and several application icons. The system tray in the bottom right corner displays the time as 08:12 and the date as 16-07-2023. A watermark in the bottom right corner reads 'Windows Server 2019 Datacenter Evaluation Windows License valid for 161 days Build 17763.rs5_release.180914-1434'.

Name	PID	Description	Status	Group
AJRouter		AllJoyn Router Service	Stopped	LocalServiceN...
ALG		Application Layer Gateway Service	Stopped	
AppIDSvc		Application Identity	Stopped	LocalServiceN...
Appinfo		Application Information	Stopped	netsvcs
AppMgmt		Application Management	Stopped	netsvcs
AppReadiness		App Readiness	Stopped	AppReadiness
AppVClient		Microsoft App-V Client	Stopped	
AppXSvc		AppX Deployment Service (AppXSVC)	Stopped	wsappx
AudioEndpointBuilder		Windows Audio Endpoint Builder	Stopped	LocalSystemN...
Audiosrv		Windows Audio	Stopped	LocalServiceN...
AxInstSV		ActiveX Installer (AxInstSV)	Stopped	AxInstSVGroup
BFE	1468	Base Filtering Engine	Running	LocalServiceN...
BITS		Background Intelligent Transfer Servi...	Stopped	netsvcs
BrokerInfrastructure	740	Background Tasks Infrastructure Ser...	Running	DcomLaunch
BTAGService		Bluetooth Audio Gateway Service	Stopped	LocalServiceN...
BthAvctpSvc		AVCTP service	Stopped	LocalService
bthserv		Bluetooth Support Service	Stopped	LocalService
camsvc		Capability Access Manager Service	Stopped	appmodel
CaptureService		CaptureService	Stopped	LocalService
CaptureService_3dae8		CaptureService_3dae8	Stopped	LocalService
cbdhsvc		Clipboard User Service	Stopped	ClipboardSvc...
cbdhsvc_3dae8		Clipboard User Service_3dae8	Stopped	ClipboardSvc...
CDPSvc	1172	Connected Devices Platform Service	Running	LocalService

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (29/0) View Help

Registry hives (1) Available bookmarks (29/0)

Find

Key name

- SafeBoot
- Services**
 - .NET CLR Data
 - .NET CLR Networking
 - .NET CLR Networking 4.0.0.0
 - .NET Data Provider for Oracle
 - .NET Data Provider for SqlServer
 - .NET Memory Cache 4.0
 - .NETFramework
 - 1394ohci
 - 3ware

Bookmark information

Hive: C:\Cases\Analysis\Registry\SYSTEM

Category: Operating system

Name: Services

Key path: ControlSet001\Services

Short description: Service definitions and parameters

Long description:

Values Services

Drag a column header here to group by that column

Name	Descri...	Display...	Start ...	Servic...	Name ...	Param...	Group	Image ...	Servic...	Require...
3ware			Boot	Kernel...	2023-0...	2019-1...	SCSI miniport	System32\drivers\3ware.sys		
AarSvc	@%SystemRoot%\system32\AarSvc.dll,-101	@%SystemRoot%\system32\AarSvc.dll,-100	Manual	96	2019-1...	2019-1...		%SystemRoot%\system32\svchost.exe -k AarSvcGroup -p	%SystemRoot%\System32\AarSvc.dll	SeImpersonatePrivilege
ACPI		@acpi.inf,%ACPI.SvcDesc%;Microsoft ACPI Driver	Boot	Kernel...	2023-0...	2023-0...	Core	System32\drivers\ACPI.sys		
AcpiDev		@acpidev.inf,%AcpiDev.	Manual	Kernel...	2019-1...		Extended Base	\SystemRoot\System32\		

Total rows: 691

Type viewer

Loaded the system hives in Registry Explorer

*C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

all x DEFAULT.txt x NTUSER.DAT.txt x SECURITY.txt x SOFTWARE.txt x SAM.txt x UsrClass.dat.txt x SYSTEM.txt x SYSTEM x

```
796 -----
797 services v.20191024
798 (System) Lists services/drivers in Services key by LastWrite times
799
800 ControlSet001\Services
801 Lists services/drivers in Services key by LastWrite times
802
803 Thu Jun 29 09:06:16 2023 Z
804     Name      = BITS
805     Display   = @%SystemRoot%\system32\qmgr.dll,-1000
806     ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs -p
807     Type      = Share_Process
808     Start     = Manual
809     Group     =
810
811 Thu Jun 29 08:15:07 2023 Z
812     Name      = WdDevFlt
813     Display   =
814     ImagePath =
815     Type      =
816     Start     =
817     Group     =
818
819 Thu Jun 29 08:14:42 2023 Z
820     Name      = WdFilter
```

Search results - (1 hit)

Search "services v." (1 hit in 1 file of 1 searched)

C:\Cases\Analysis\Registry\SYSTEM.txt (1 hit)

Line 797: services v.20191024

Normal text file | length : 3,69,812 | lines : 7,102 | Ln : 5,612 | Col : 25 | Pos : 1,93,255 | Windows (CR LF) | UTF-8 | INS

08:03 16-07-2023

System hives edit with Notepad++ and Find the services on target system and show the given output.

Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>schtasks

Folder: \	TaskName	Next Run Time	Status
=====	=====	=====	=====
User_Feed_Synchronization-{6C5B0DEF-65CE		16-07-2023 11:05:14	Ready

Folder: \Microsoft	TaskName	Next Run Time	Status
=====	=====	=====	=====
INFO: There are no scheduled tasks presently available at your access level.			

Folder: \Microsoft\Windows	TaskName	Next Run Time	Status
=====	=====	=====	=====
INFO: There are no scheduled tasks presently available at your access level.			

Folder: \Microsoft\Windows\.NET Framework	TaskName	Next Run Time	Status
=====	=====	=====	=====
.NET Framework NGEN v4.0.30319		N/A	Ready
.NET Framework NGEN v4.0.30319 64		N/A	Ready
.NET Framework NGEN v4.0.30319 64 Critic		N/A	Disabled
.NET Framework NGEN v4.0.30319 Critical		N/A	Disabled

Folder: \Microsoft\Windows\Active Directory Rights Management Services Client	TaskName	Next Run Time	Status
=====	=====	=====	=====
AD RMS Rights Policy Template Management		N/A	Disabled
AD RMS Rights Policy Template Management		N/A	Ready

Folder: \Microsoft\Windows\AppID	TaskName	Next Run Time	Status
=====	=====	=====	=====

Open cmd as a
Administrator and
type this
command.



08:50
16-07-2023



C:\Cases\Analysis\Registry\SOFTWARE.txt - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

all x DEFAULT.txt x NTUSER.DAT.txt x SECURITY.txt x SOFTWARE.txt x SAM.txt x UsrClass.dat.txt x SYSTEM.txt x SYSTEM x

```
40484
40485 9 - LastWrite time: 2023-06-28 16:32:41Z
40486 Path: file:///C:\[af17ba98-35d5-43f9-a08a-ffba85076e9d]\Users\
40487
40488 -----
40489 taskcache v.20200427
40490 (Software) Checks TaskCache\Tree root keys (not subkeys)
40491
40492 MicrosoftEdgeUpdateTaskMachineCore
40493 LastWrite: 2023-06-28 16:05:57Z
40494 Id: {C32E8E08-558A-4F92-BAE5-3BEFEFE1827B}
40495 Task Reg Time: 2023-06-28 16:05:57Z
40496 Task Last Run: 2023-06-29 08:08:14Z
40497 Task Completed: 2023-06-29 08:08:19Z
40498
40499 MicrosoftEdgeUpdateTaskMachineUA
40500 LastWrite: 2023-06-28 16:05:57Z
40501 Id: {D30B1923-95AE-4E7C-9FFD-E4D35696027C}
40502 Task Reg Time: 2023-06-28 16:05:57Z
40503 Task Last Run: 2023-06-29 08:12:26Z
40504 Task Completed: 2023-06-29 08:12:32Z
40505
40506 OneDrive Reporting Task-S-1-5-21-3331464962-214784631-3394824829-1001
40507 LastWrite: 2023-06-28 16:25:12Z
40508 Id: {FB7019CD-AADF-4803-AE0C-148AD2A4DDF1}
```

Open the software hives with Notepad++ and search taskcache and show this Result.

Search results - (3 hits)

- Line 40489: taskcache v.20200427
- Line 40490: (Software) Checks TaskCache\Tree root keys (not subkeys)
- Line 40520: (Software) Checks TaskCache\Tasks subkeys

Search "task cache" (0 hits in 0 files of 9 searched)

Normal text file length: 25,34,532 lines: 41,650 Ln: 40,489 Col: 10 Sel: 9 | 1 Windows (CR LF) UTF-8 INS

08:53 16-07-2023

Analysis with Sysinternals Autorun tool

[Autoruns for Windows - Sysinternals | Microsoft Learn](https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns)

The screenshot shows the Microsoft Learn page for the Sysinternals Autoruns tool. On the left, there is a navigation menu with categories like 'Downloads', 'Process Utilities', and 'AutoRuns'. The main content area includes a 'Usage' section, a 'Download' link, and a 'By Mark Russinovich' section. A blue-bordered box highlights the download information: 'Published: June 27, 2023', 'Download Autoruns and Autorunsc (2.8 MB)', and 'Run now from Sysinternals Live'. Below this, a preview of the Autoruns tool interface is shown, displaying a list of autorun entries with columns for Name, Description, Publisher, and Image Path.

Usage
Autorunsc Usage
Related Links
Download

By Mark Russinovich

Published: June 27, 2023

[Download Autoruns and Autorunsc](#) (2.8 MB)
[Run now from Sysinternals Live](#).

Name	Description	Publisher	Image Path
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
com.squirrel.Teams.Teams	Microsoft Teams	(Verified) Microsoft 3rd Party Appli..	C:\Users\marich\AppData\Local\MicrosoftTe
MicrosoftEdgeAutoLaunch_806225252049304893A664A717F81932	Microsoft Edge	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Appli
OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Program Files\Microsoft OneDrive\OneDri
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
TechSmithSnagit	Snagit	(Verified) TechSmith Corporation	C:\Program Files\TechSmith\Snagit_2020\Snag
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce			
Delete Cached Standalone Update Binary	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe
Delete Cached Update Binary	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
Microsoft Edge	Microsoft Edge Installer	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Appli

Autorun tools use for detect and Analyze the autorun file like malware and virus Affected file , run file with boot time etc.

Download the tool from microsoft

File Explorer window showing the contents of the 'Aautoruns' folder in the 'Downloads' directory. The 'Aautoruns64' file is selected, and the context menu is open, highlighting the 'Run as administrator' option.

Name	Date modified	Type	Size
autoruns	27-06-2023 16:55	Compiled HTML ...	25 KB
Aautoruns	27-06-2023 16:55	Application	1,742 KB
Aautoruns64	27-06-2023 16:55	Application	1,934 KB
Aut...	2023 16:55	Application	2,040 KB
aut...	2023 16:55	Application	702 KB
aut...	2023 16:55	Application	785 KB
aut...	2023 16:55	Application	808 KB
Eul...	2023 16:54	Text Document	8 KB

Open the tool as run Administrator

File Search Entry User Options Category Help

- Open... Ctrl+O
- Save... Ctrl+S
- Analyze Offline System...
- Compare...
- Refresh F5
- Cancel ESC
- Exit

Image Hijacks	Applnit	Known DLLs	Winlogon	Winsock Providers	Print Monitors
Logon	Explorer	Internet Explorer	Scheduled Tasks	Services	Drivers
Description		Publisher	Image Path		
Set\Control\SafeBoot\AlternateShell					
Windows Command Processor		(Verified) Microsoft Windows	C:\Windows\system32\cmd.e		
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells					
<input checked="" type="checkbox"/>	30000	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.e	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components					
<input checked="" type="checkbox"/>	n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscor	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components					
<input checked="" type="checkbox"/>	n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscor	
Task Scheduler					
<input checked="" type="checkbox"/>	\Microsoft\Windows\Server Manager\CleanupOldPerfLogs	Microsoft © Console Based Script Host	(Verified) Microsoft Windows	C:\Windows\system32\cscript	
<input type="checkbox"/>	\Microsoft\Windows\Software Inventory Logging\Collection	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.e	

Offline System

Select the directories of the offline system:

System Root: ...

User Profile: ...

OK Cancel

	Publisher	Image Path
<input checked="" type="checkbox"/> <input type="checkbox"/> MicrosoftEdgeAutoLaunch_1ED6AFCC191394652DA0C4ECFC73...	Microsoft Edge	(Verified) Microsoft Corporation C:\Program Files (x86)\Micros
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation C:\Users\Denisha\AppData\Lc
<input checked="" type="checkbox"/> HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms		
<input checked="" type="checkbox"/> rdpclip	RDP Clipboard Monitor	(Not Verified) Microsoft Corporati... C:\Windows\system32\rdpclip
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		
<input checked="" type="checkbox"/> SecurityHealth	Windows Security notification icon	(Not Verified) Microsoft Corporati... C:\Windows\system32\Securi
<input checked="" type="checkbox"/> VBoxTray	VirtualBox Guest Additions Tray Applicati...	(Not Verified) Oracle and/or its aff... C:\Windows\system32\VBoxT
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell		
<input checked="" type="checkbox"/> explorer.exe	Windows Explorer	(Not Verified) Microsoft Corporati... C:\Windows\explorer.exe
<input checked="" type="checkbox"/> HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell		
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Not Verified) Microsoft Corporati... C:\Windows\system32\cmd.e
<input checked="" type="checkbox"/> HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit		
<input checked="" type="checkbox"/> C:\Windows\system32\userinit.exe	Userinit Logon Application	(Not Verified) Microsoft Corporati... C:\Windows\system32\userin

OneDrive

Microsoft OneDrive

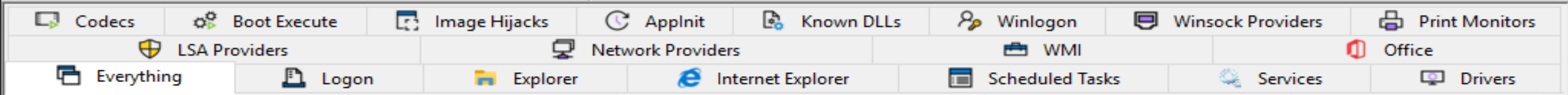
(Verified) Microsoft Corporation

Size: 2,311 K

Time: 28-06-2023 16:25

Version: 21.220.1024.0005

"C:\Users\Denisha\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background



Autoruns Entry	Description	Publisher	Image Path
Logon			
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> MicrosoftEdgeAutoLaunch_1ED6AFCC191394652DA0C4ECFC73...	Microsoft Edge	(Verified) Microsoft Corporation	C:\Program Files (x86)\Micros
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Users\Denisha\AppData\Lo
HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms			
<input checked="" type="checkbox"/> rdpclip	RDP Clipboard Monitor	(Not Verified) Microsoft Corporati...	C:\Windows\system32\rdpcli
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> SecurityHealth	Windows Security notification icon	(Not Verified) Microsoft Corporati...	C:\Windows\system32\Securi
<input checked="" type="checkbox"/> VBoxTray	VirtualBox Guest Additions Tray Applicati...	(Not Verified) Oracle and/or its aff...	C:\Windows\system32\VBoxT
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell			
<input checked="" type="checkbox"/> explorer.exe	Windows Explorer	(Not Verified) Microsoft Corporati...	C:\Windows\explorer.exe
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Not Verified) Microsoft Corporati...	C:\Windows\system32\cmd.e
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit			
<input checked="" type="checkbox"/> C:\Windows\system32\userinit.exe	Userinit Logon Application	(Not Verified) Microsoft Corporati...	C:\Windows\system32\userin

OneDrive
 Microsoft OneDrive
 (Verified) Microsoft Corporation
 "C:\Users\Denisha\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background

Size: 2,311 K
 Time: 28-06-2023 16:25
 Version: 21.220.1024.0005

Show all autoruns file like malware , virus file , boot load file.



Event log Analysis

The main purpose of the event logs is to provide information to administrators and users. They are structured in five levels (information, warning, error, critical, and success/failure audit). In terms of forensic analysis, this is a valuable source to understand the course of actions on a system.

Encyclopedia

- Event IDs
- All Event IDs
- Audit Policy

Go To Event ID:

Security Log Quick Reference Chart



Download now!

← Windows Security Log Event ID 4624 →

4624: An account was successfully logged on

On this page

- Description of this event
- Field level details
- Examples
- Discuss this event
- Mini-seminars on this event

This is a highly valuable event since it documents each and every successful attempt to logon to the local computer regardless of logon type, location of the user or type of account. You can tie this event to logoff events 4634 and 4647 using Logon ID.

Win2012 adds the Impersonation Level field as shown in the example.

Win2016/10 add further fields explained below.

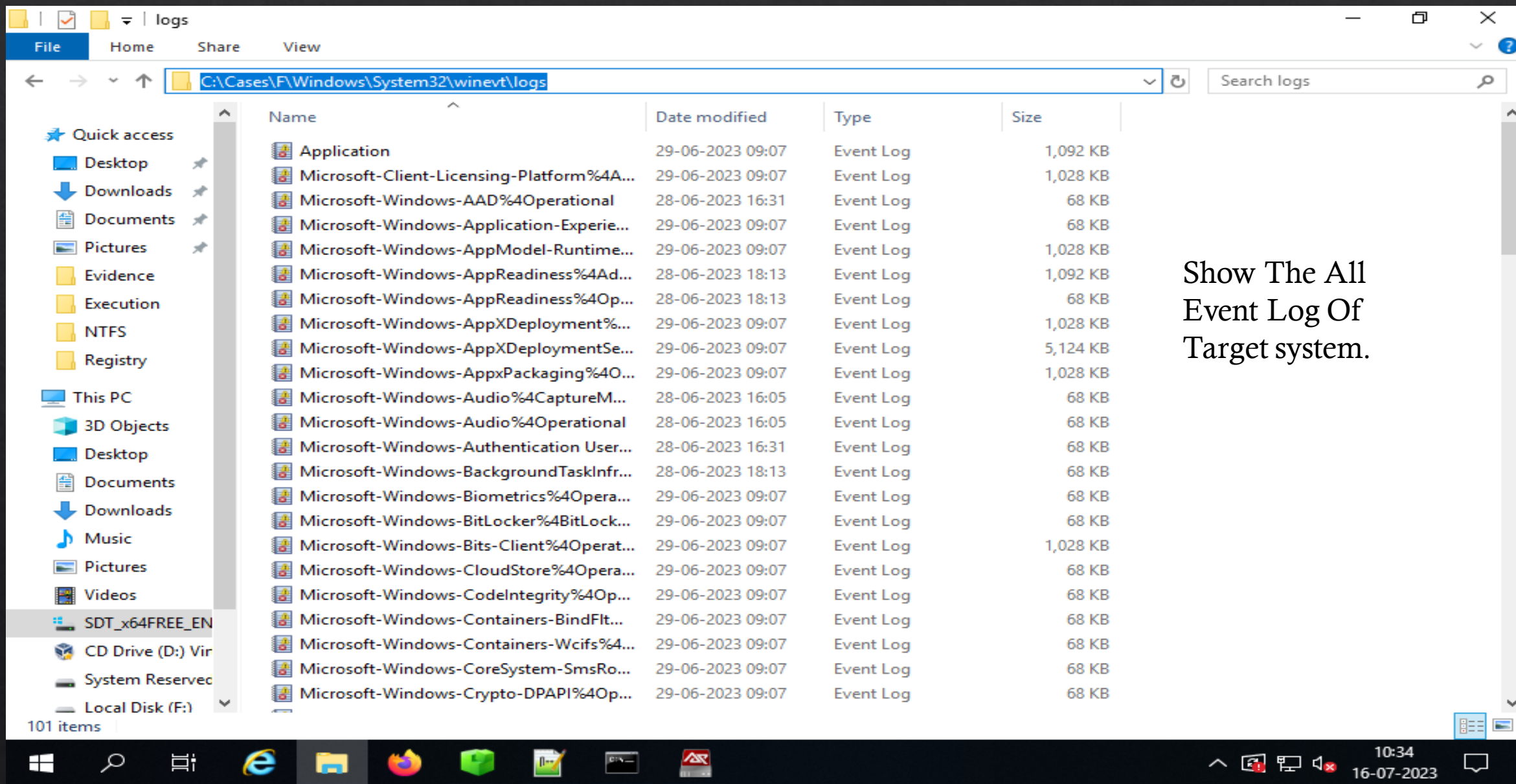
Free Security Log Resources by Randy

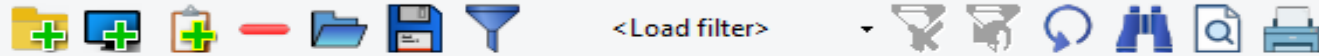
- Free Security Log Quick Reference Chart
- Windows Event Collection: Supercharger Free Edition
- Free Active Directory Change Auditing Solution
- Free Course: Security Log Secrets

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022
Category • Subcategory	Logon/Logoff • Logon
Type	Success
Corresponding events in Windows 2003 and before	528 , 540

Enter the event ID and show the detail.

Analyzing Windows event logs with EventLogExplorer and EvtxCmd





Objects tree

Search

- > WIN-AJDB7GOIQ
- > Log Files
- > Task templates

Open the Event log explorer and load the first event.

Application.evtx

291 1 UTC

	Date	Time	Event	Source	Category	User	Computer
tion	29-06-2023	08:14:51	16384	Microsoft-Windows	None	N/A	DESKTOP-MD2HCPT
tion	29-06-2023	08:13:57	15	SecurityCenter	None	N/A	DESKTOP-MD2HCPT
tion	29-06-2023	08:13:25	15	SecurityCenter	None	N/A	DESKTOP-MD2HCPT
tion	29-06-2023	08:12:33	16394	Microsoft-Windows	None	N/A	DESKTOP-MD2HCPT
tion	29-06-2023	08:12:32	0	edgeupdate	None	N/A	DESKTOP-MD2HCPT
tion	29-06-2023	08:11:49	16384	Microsoft-Windows	None	N/A	DESKTOP-MD2HCPT
tion	29-06-2023	08:09:53	16394	Microsoft-Windows	None	N/A	DESKTOP-MD2HCPT
tion	29-06-2023	08:09:45	16384	Microsoft-Windows	None	N/A	DESKTOP-MD2HCPT
tion	29-06-2023	08:08:16	16394	Microsoft-Windows	None	N/A	DESKTOP-MD2HCPT
tion	29-06-2023	08:08:11	15	SecurityCenter	None	N/A	DESKTOP-MD2HCPT
tion	29-06-2023	08:08:08	15	SecurityCenter	None	N/A	DESKTOP-MD2HCPT
tion	29-06-2023	08:06:55	16384	Microsoft-Windows	None	N/A	DESKTOP-MD2HCPT
tion	29-06-2023	08:06:07	16394	Microsoft-Windows	None	N/A	DESKTOP-MD2HCPT
tion	29-06-2023	08:05:42	16384	Microsoft-Windows	None	N/A	DESKTOP-MD2HCPT

Description

The description for Event ID (15) in Source (SecurityCenter) could not be found. Either the component that raises this event is not installed on the computer or the installation is corrupted. You can install or repair the component or try to change Description Server.

The following information was included with the event:
Windows Defender

Description Data

Get-ZimmermanTools

File Home Share View

C:\Tools\Get-ZimmermanTools

Search Get-ZimmermanTools

Name	Date modified	Type	Size
EvtxECmd	28-06-2023 13:40	File folder	
EZViewer	28-06-2023 13:40	File folder	
Hasher	28-06-2023 13:41	File folder	
iisGeolocate	28-06-2023 13:44	File folder	
JumpListExplorer	28-06-2023 13:41	File folder	
MFTExplorer	28-06-2023 13:41	File folder	
RECmd	28-06-2023 13:41	File folder	
RegistryExplorer	28-06-2023 13:42	File folder	
SDBExplorer	28-06-2023 13:42	File folder	
ShellBagsExplorer	01-07-2023 10:36	File folder	
SQLCmd	28-06-2023 13:43	File folder	
TimelineExplorer	01-07-2023 05:43	File folder	
XWFIM	28-06-2023 13:44	File folder	
!!!RemoteFileDetails	28-06-2023 13:44	CSV File	5 KB
AmcacheParser	21-05-2023 11:49	Application	4,661 KB
AppCompatCacheParser	07-03-2023 15:13	Application	4,523 KB
bstrings	20-05-2022 12:38	Application	3,997 KB
ChangeLog	28-06-2023 13:44	Text Document	33 KB
Get-ZimmermanTools	18-05-2023 14:24	Windows PowerS...	24 KB
JLECmd	13-03-2023 17:06	Application	4,792 KB
LECmd	04-03-2023 10:30	Application	5,063 KB
MFTECmd	20-10-2022 13:37	Application	4,409 KB
PECmd	28-01-2022 12:08	Application	3,885 KB

32 items | 1 item selected

Open the command base EvtxECmd.

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Tools\Get-ZimmermanTools\EvtxECmd>EvtxECmd.exe
Description:
  EvtxECmd version 1.5.0.0

  Author: Eric Zimmerman (saericzimmerman@gmail.com)
  https://github.com/EricZimmerman/evt

Examples: EvtxECmd.exe -f "C:\Temp\Application.evtx" --csv "c:\temp\out" --csvf MyOutputFile.csv
  EvtxECmd.exe -f "C:\Temp\Application.evtx" --csv "c:\temp\out"
  EvtxECmd.exe -f "C:\Temp\Application.evtx" --json "c:\temp\jsonout"

Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes

Usage:
  EvtxECmd [options]

Options:
  -f <f>      File to process. This or -d is required
  -d <d>      Directory to process that contains evt files. This or -f is required
  --csv <csv> Directory to save CSV formatted results to
  --csvf <csvf> File name to save CSV formatted results to. When present, overrides default name
  --json <json> Directory to save JSON formatted results to
  --jsonf <jsonf> File name to save JSON formatted results to. When present, overrides default name
  --xml <xml> Directory to save XML formatted results to
  --xmlf <xmlf> File name to save XML formatted results to. When present, overrides default name
  --dt <dt>   The custom date/time format to use when displaying time stamps [default: yyyy-MM-dd HH:mm:ss.fffffff]
  --inc <inc> List of Event IDs to process. All others are ignored. Overrides --exc Format is 4624,4625,5410
```

The following information was included with the event:
Windows Defender

Description	Data
-------------	------

```

--fj           When true, export all available data when using --json [default: False]
--tdt <tdt>   The number of seconds to use for time discrepancy detection [default: 1]
--met         When true, show metrics about processed event log [default: True]
--maps <maps> The path where event maps are located. Defaults to 'Maps' folder where program was executed
              [default: C:\Tools\Get-ZimmermanTools\EvtxECmd\Maps]
--vss        Process all Volume Shadow Copies that exist on drive specified by -f or -d [default: False]
--dedupe     Deduplicate -f or -d & VSCs based on SHA-1. First file found wins [default: True]
--sync       If true, the latest maps from https://github.com/EricZimmerman/evtx/tree/master/evtx/Maps are
              downloaded and local maps updated [default: False]
--debug      Show debug information during processing [default: False]
--trace      Show trace information during processing [default: False]
--version    Show version information
-?, -h, --help Show help and usage information

```

Create the Event log folder in Analysis folder then After this command is execute.

-f or -d is required. Exiting

```
C:\Tools\Get-ZimmermanTools\EvtxECmd>EvtxECmd.exe -d C:\Cases\F\Windows\System32\winevt\logs --csv C:\Cases\Analysis\Eventlogs
```

EvtxECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
<https://github.com/EricZimmerman/evtx>

Command line: -d C:\Cases\F\Windows\System32\winevt\logs --csv C:\Cases\Analysis\Eventlogs

CSV output will be saved to C:\Cases\Analysis\Eventlogs\20230716112553_EvtxECmd_Output.csv

Error loading map file C:\Tools\Get-ZimmermanTools\EvtxECmd\Maps\Microsoft-Windows-Storage-ClassPnP-Operational_Microsoft

The following information was included with the event:
 Windows Defender

Description Data

Eventlogs

File Home Share View

C:\Cases\Analysis\Eventlogs

Search Eventlogs

Name	Date modified	Type	Size
20230716112553_EvtxECmd_Output	16-07-2023 11:26	CSV File	28,480 KB

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- Evidence
- Execution
- NTFS
- Registry

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- SDT_x64FREE_EN
- CD Drive (D:) Vir
- System Reserved
- Local Disk (F:)

1 item

Show the all event output in this file

11:28
16-07-2023

20230716112553_EvtxECmd_Output.csv

Drag a column header here to group by that column

Enter text to search...

Find

	Line	Tag	Record Number	Event Record Id	Time Created	Event Id	Level	Provider
Y	=	<input checked="" type="checkbox"/>	=	=	=	=	RB	RB
	175	<input type="checkbox"/>	175	175	2023-06-28 16...	15	Info	SecurityCenter
	176	<input type="checkbox"/>	176	176	2023-06-28 16...	16394	Info	Microsoft-Windows-Security-
	177	<input type="checkbox"/>	177	177	2023-06-28 16...	15	Info	SecurityCenter
	178	<input type="checkbox"/>	178	178	2023-06-28 16...	15	Info	SecurityCenter
	179	<input type="checkbox"/>	179	179	2023-06-28 16...	15	Info	SecurityCenter
	180	<input type="checkbox"/>	180	180	2023-06-28 16...	16384	Info	Microsoft-Windows-Security-
	181	<input type="checkbox"/>	181	181	2023-06-28 16...	16394	Info	Microsoft-Windows-Security-
	182	<input type="checkbox"/>	182	182	2023-06-28 16...	16384	Info	Microsoft-Windows-Security-
	183	<input type="checkbox"/>	183	183	2023-06-28 16...	8224	Info	VSS
	184	<input type="checkbox"/>	184	184	2023-06-28 16...	16394	Info	Microsoft-Windows-Security-
	185	<input type="checkbox"/>	185	185	2023-06-28 16...	1034	Info	Microsoft-Windows-Security-
	186	<input type="checkbox"/>	186	186	2023-06-28 16...	1033	Info	Microsoft-Windows-Security-
	187	<input type="checkbox"/>	187	187	2023-06-28 16...	16384	Info	Microsoft-Windows-Security-
	188	<input type="checkbox"/>	188	188	2023-06-28 16...	1001	Info	Windows Error Reporting
	189	<input type="checkbox"/>	189	189	2023-06-28 16...	15	Info	SecurityCenter
	190	<input type="checkbox"/>	190	190	2023-06-28 17...	16394	Info	Microsoft-Windows-Security-
	191	<input type="checkbox"/>	191	191	2023-06-28 17...	16384	Info	Microsoft-Windows-Security-
	192	<input type="checkbox"/>	192	192	2023-06-28 17...	1001	Info	Windows Error Reporting
	193	<input type="checkbox"/>	193	193	2023-06-28 17...	1001	Info	Windows Error Reporting

1. Windows Event Logs Defender Analysis

Source

Microsoft-Windows-Windows Defender

Event IDs

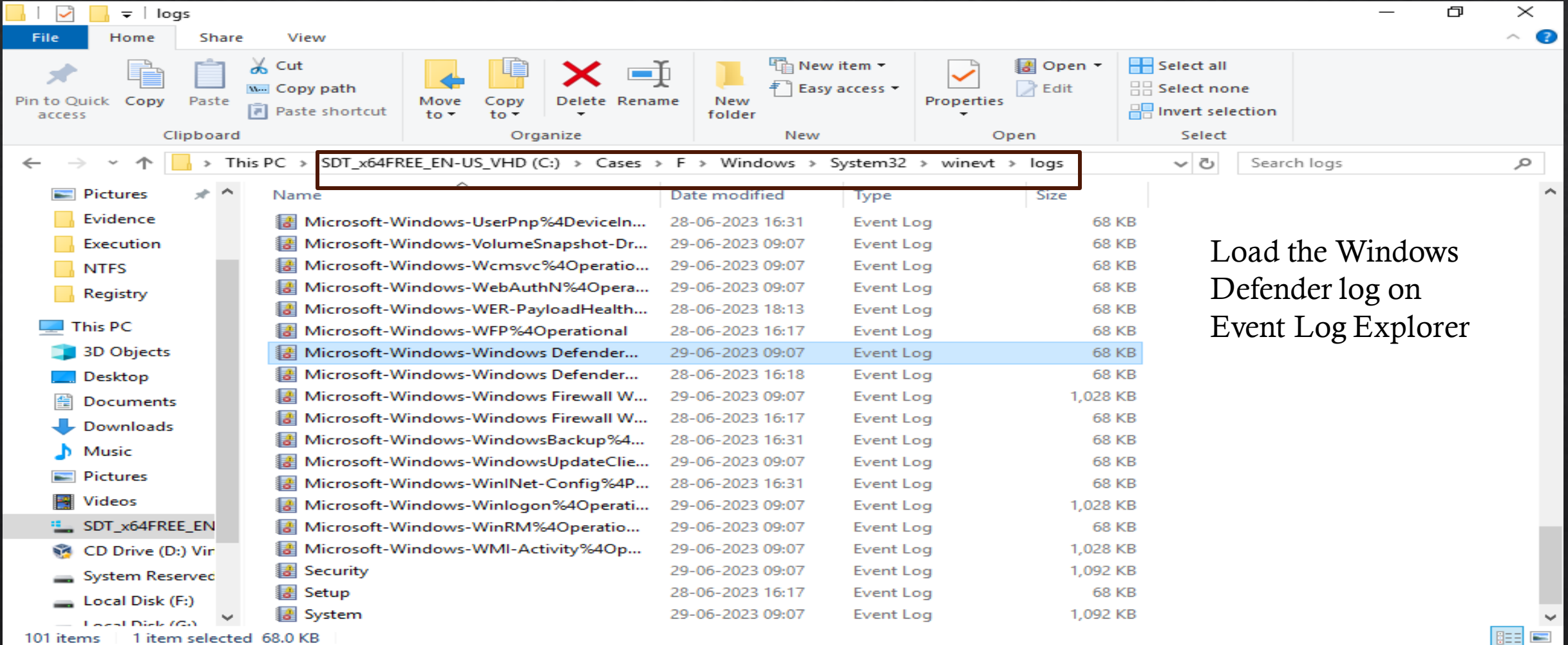
5000

Description

Defender enabled

5001

Defender disabled



Load the Windows Defender log on Event Log Explorer

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Microsoft-Windows-Windows Defender%4Operational.evtx

UTC

Type	Date	Time	Event	Source	Category	User	Computer
Information	29-06-2023	08:15:09	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:09	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:09	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:09	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:09	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I
Information	29-06-2023	08:15:07	5007	Microsoft-Windows	None	\SYSTEM	DESKTOP-I

Description

Microsoft Defender Antivirus Configuration has changed. If this is an unexpected event you should review the settings as this may be the result of malware.

Old value: Default\Features\TamperProtectionSource = 0x0
New value: HKLM\SOFTWARE\Microsoft\Windows Defender\Features\TamperProtectionSource = 0x5

Description Data

12:41
16-07-2023

Show the output of windows defender log.

Filter

Apply filter to:
 Active event log view (File: C:\Cases\F\Windows\System32\winevt\logs\Microsoft-Wind
 Event log view(s) on your choice

Event types

- Verbose
- Information
- Warning
- Error
- Critical
- Audit Success
- Audit Failure

Source: ... Exclude

Category: ... Exclude

User: ... Exclude

Computer: ... Exclude

Event ID(s): Exclude
Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450! 10,255)

Text in description: RegExp Exclude

Date Time Separately

From: To: Exclude

Display event for the last days hours Exclude

Custom columns **Description params**

Name	Operator	Value
Custom column 1		
Custom column 2		
Custom column 3		
Custom column 4		
Custom column 5		

Clear Load... Save... **OK** Cancel

Untitled.ELX - Event Log E

File Database Tree Log

Objects tree

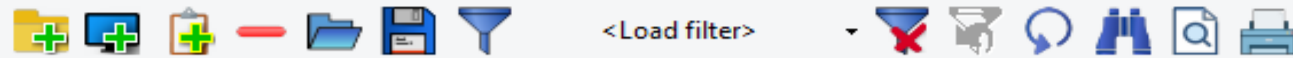
Search

- WIN-AJDB7GOIQ
- Log Files
- Task templates

Filter the Particular log as your requiremet

- Computer
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I
- DESKTOP-I

may be the result of



Objects tree

- > WIN-AJDB7GOIQ
- > Log Files
- > Task templates

Microsoft-Windows-Windows Defender%4Operational.evtx

UTC

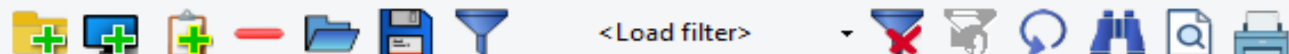
57 4 1

Type	Date	Time	Event	Source	Category	User	Computer
Information	29-06-2023	08:02:07	5000	Microsoft-Windows	None	\SYSTEM	DESKTOP-M
Information	28-06-2023	16:47:04	5001	Microsoft-Windows	None	\SYSTEM	DESKTOP-M
Information	28-06-2023	16:32:14	5000	Microsoft-Windows	None	\SYSTEM	DESKTOP-M
Information	28-06-2023	16:28:01	5001	Microsoft-Windows	None	\SYSTEM	DESKTOP-M

Description

Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was enabled.

Description Data



Objects tree

- > WIN-AJDB7GOIQ
- > Log Files
- > Task templates

Microsoft-Windows-Windows Defender%4Operational.evtx

UTC
 57 4 1

Type	Date	Time	Event	Source	Category	User	Computer
Information	29-06-2023	08:02:07	5000	Microsoft-Windows	None	\SYSTEM	DESKTOP-M
Information	28-06-2023	16:47:04	5001	Microsoft-Windows	None	\SYSTEM	DESKTOP-M
Information	28-06-2023	16:32:14	5000	Microsoft-Windows	None	\SYSTEM	DESKTOP-M
Information	28-06-2023	16:28:01	5001	Microsoft-Windows	None	\SYSTEM	DESKTOP-M

Description

Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.

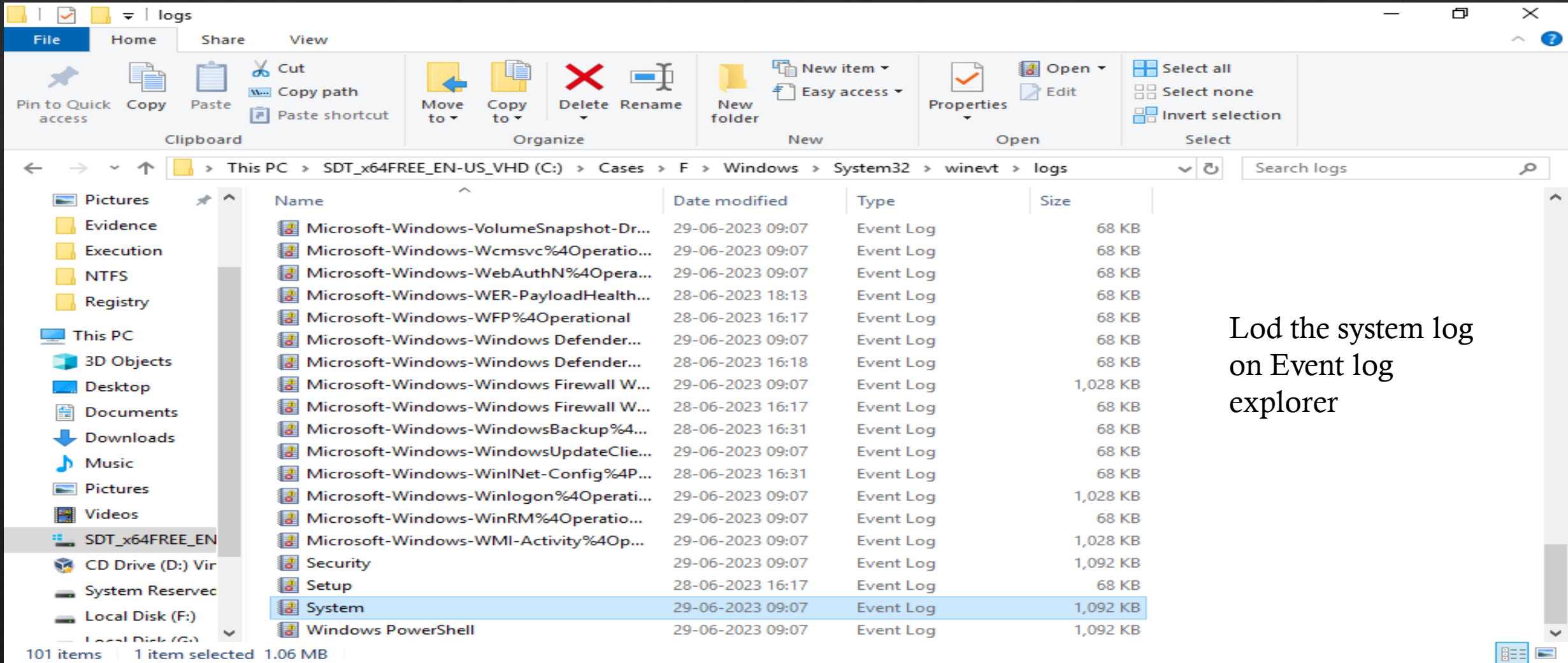
Description Data

2. System log Analysis

Source System

Event IDs
7045

Description
A new service was installed



Lod the system log on Event log explorer

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

<Load filter>

Objects tree

System.evtx

818 1 UTC

Type	Date	Time	Event	Source	Category	User
Information	29-06-2023	09:07:51	50037	Microsoft-Windows	Service State Event	NT AUTHORITY\LOCAL SERVICE
Information	29-06-2023	09:07:51	50106	Microsoft-Windows	Service State Event	NT AUTHORITY\LOCAL SERVICE
Information	29-06-2023	09:07:50	51057	Microsoft-Windows	Service State Event	NT AUTHORITY\LOCAL SERVICE
Information	29-06-2023	09:07:50	51047	Microsoft-Windows	Service State Event	NT AUTHORITY\LOCAL SERVICE
Information	29-06-2023	09:07:50	50105	Microsoft-Windows	Service State Event	NT AUTHORITY\LOCAL SERVICE
Information	29-06-2023	09:07:50	50104	Microsoft-Windows	Service State Event	NT AUTHORITY\LOCAL SERVICE
Information	29-06-2023	09:07:51	6006	EventLog	None	N/A
Information	29-06-2023	09:07:48	7002	Microsoft-Windows	(1102)	\SYSTEM
Information	29-06-2023	09:07:41	1074	User32	None	\S-1-5-21-3331464962-214784631-33
Information	29-06-2023	09:06:16	7040	Service Control Mar	None	\SYSTEM
Information	29-06-2023	09:04:23	7040	Service Control Mar	None	\SYSTEM
Information	29-06-2023	08:27:44	16	Microsoft-Windows	None	\SYSTEM
Information	29-06-2023	08:27:08	19	Microsoft-Windows	Windows Update Age	\SYSTEM
Information	29-06-2023	08:27:06	16	Microsoft-Windows	None	\S-1-5-21-3331464962-214784631-33
Information	29-06-2023	08:27:06	43	Microsoft-Windows	Windows Update Age	\SYSTEM
Information	29-06-2023	08:27:03	16	Microsoft-Windows	None	\SYSTEM

Description

DHCPv4 client service is stopped. ShutDown Flag value is 1

Description Data

Click
this icon



Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

System.evtx

818 10 1 UTC

Time	Event	Source	Category	User	Computer
16:58:13	7045	Service Control Mar	None	\S-1-5-21-3331464962-214784631-3394824829-1001	DESKTOP-MD2HCPT
16:58:13	7045	Service Control Mar	None	\S-1-5-21-3331464962-214784631-3394824829-1001	DESKTOP-MD2HCPT
16:30:52	7045	Service Control Mar	None	\S-1-5-21-3331464962-214784631-3394824829-1001	DESKTOP-MD2HCPT
16:30:52	7045	Service Control Mar	None	\S-1-5-21-3331464962-214784631-3394824829-1001	DESKTOP-MD2HCPT
16:30:51	7045	Service Control Mar	None	\S-1-5-21-3331464962-214784631-3394824829-1001	DESKTOP-MD2HCPT
16:30:46	7045	Service Control Mar	None	\SYSTEM	DESKTOP-MD2HCPT
16:30:43	7045	Service Control Mar	None	\SYSTEM	DESKTOP-MD2HCPT
16:07:49	7045	Service Control Mar	None	\SYSTEM	WIN-SMB9MDN3Q04
16:06:25	7045	Service Control Mar	None	\SYSTEM	WIN-SMB9MDN3Q04
16:05:21	7045	Service Control Mar	None	\SYSTEM	WIN-SMB9MDN3Q04

Description

A service was installed in the system.

Service Name: Sysmon
 Service File Name: C:\Windows\Sysmon.exe
 Service Type: user mode service
 Service Start Type: auto start
 Service Account: LocalSystem

Description about the attack script.

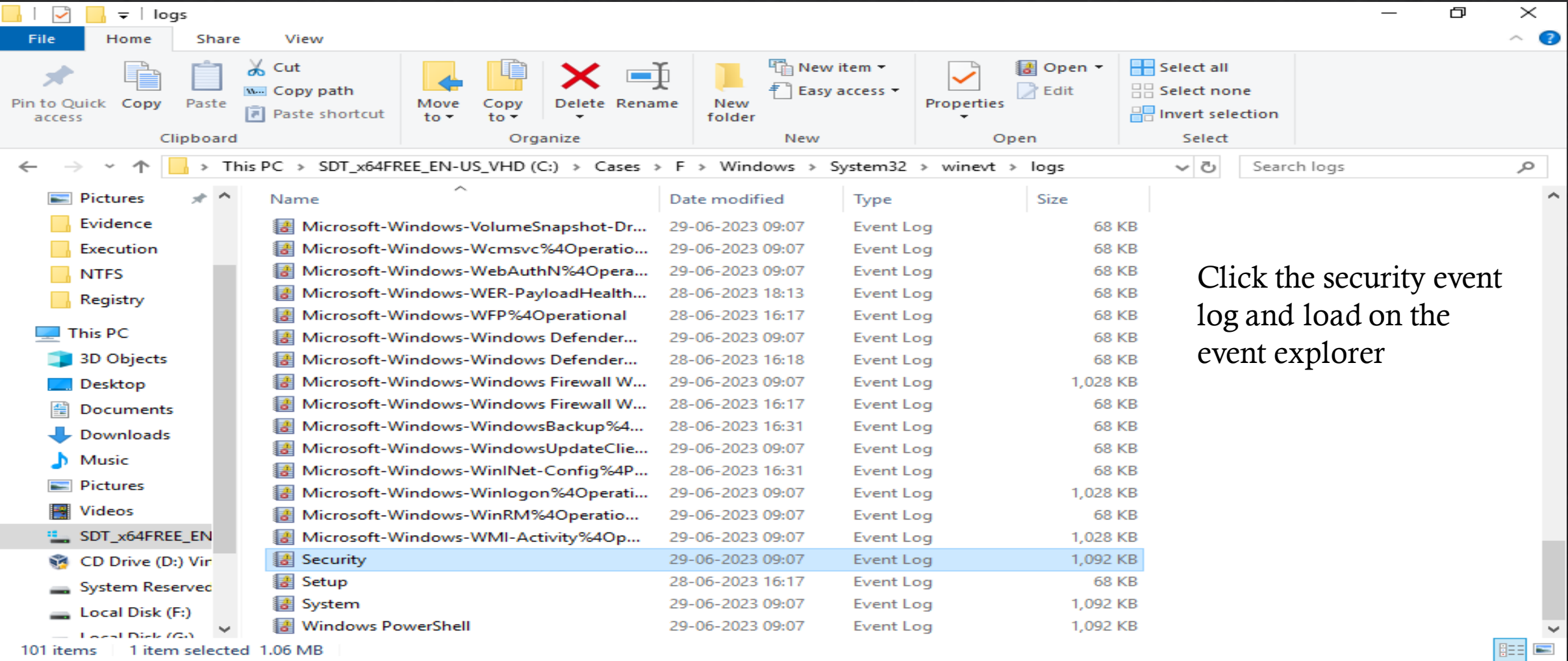
Description Data

3. Security and Authentication Event logs

Source
Security

Event IDs
4624

Description
An account was successfully logged on



Click the security event log and load on the event explorer

Untitled.ELX - Event Log Explorer

File Database Tree Log View **Event** Advanced Window Help

Objects tree

Security.evtx

1161 1 UTC

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	29-06-2023	09:07:51	1100	Microsoft-Windows	Service shutdown	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	09:07:48	4798	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	09:07:48	4798	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	09:07:48	4798	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	09:07:48	4798	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	09:07:48	4798	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	09:07:46	4647	Microsoft-Windows	Logoff	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	09:04:27	4799	Microsoft-Windows	Security Group Manag	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	09:04:27	4799	Microsoft-Windows	Security Group Manag	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	09:03:19	4672	Microsoft-Windows	Special Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	09:03:19	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	08:46:45	4672	Microsoft-Windows	Special Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	08:46:45	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	08:32:32	4672	Microsoft-Windows	Special Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	08:32:32	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	08:27:36	4672	Microsoft-Windows	Special Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	08:27:36	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	08:16:45	4672	Microsoft-Windows	Special Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	08:16:45	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H

Description

An account was successfully logged on.

Subject:

Click this icon for filter the event id

Untitled.ELX - Event Log Explorer

File Database Tree Log

Objects tree

Search

- WIN-AJDB7GOIQ
- Log Files
- Task templates

Fill the event id and description as per requirement

Filter

Apply filter to:

- Active event log view (File: C:\Cases\F\Windows\System32\winevt\logs\Security.evtx)
- Event log view(s) on your choice

Event types

- Verbose
- Information
- Warning
- Error
- Critical
- Audit Success
- Audit Failure

Source: ... Exclude

Category: ... Exclude

User: ... Exclude

Computer: ... Exclude

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description: RegExp Exclude

Date Time Separately

From: To: Exclude

Display event for the last days hours Exclude

Custom columns Description params

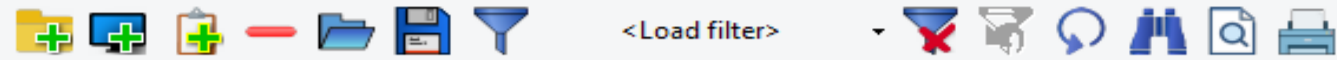
Name	Operator	Value
Custom column 1		
Custom column 2		
Custom column 3		
Custom column 4		
Custom column 5		

Clear Load... Save... OK Cancel

Computer

- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H

is the Server service, or a



Objects tree

Search

- WIN-AJDB7GOIQ
- Log Files
- Task templates

Security.evtx

1161 170 0 UTC

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	29-06-2023	09:03:19	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	08:46:45	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	08:32:32	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	08:27:36	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	08:16:45	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H
Audit Success	29-06-2023	08:14:34	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H

Description

An account was successfully logged on.

Subject:

- Security ID: S-1-5-18
- Account Name: DESKTOP-MD2HCPT\$
- Account Domain: WORKGROUP
- Logon ID: 0x3e7

Logon Information:

- Logon Type: 5
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:

- Security ID: S-1-5-18
- Account Name: SYSTEM

Show the all detail about this event log.

Description Data

4. Authentication & Logon IDs logs

4624 event id use for login detail which by filtering we can see all login details same but same time same login details have different login id. If the event log is viewed by filtering the login ID , it will show any Malicious activity like user joined a Administrator group, Any user is created , Any other user change the credential details etc.

Untitled.ELX - Event Log Explorer

File Database Tree Log

Objects tree

Search

- WIN-AJDB7GOIQ
- Log Files
- Task templates

Filter with
login ID

Filter

Apply filter to:

- Active event log view (File: C:\Cases\F\Windows\System32\winevt\logs\Security.evtx)
- Event log view(s) on your choice

Event types

- Verbose
- Information
- Warning
- Error
- Critical
- Audit Success
- Audit Failure

Source: Exclude

Category: Exclude

User: Exclude

Computer: Exclude

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description: RegExp Exclude

Date Time Separately

From: To: Exclude

Display event for the last days hours Exclude

Custom columns Description params

Name	Operator	Value
Custom column 1		
Custom column 2		
Custom column 3		
Custom column 4		
Custom column 5		

Clear Load... Save... OK Cancel

Computer

- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H
- DESKTOP-MD2H

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search

Security.evtx

UTC

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	28-06-2023	16:19:55	4648	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H
Audit Success	28-06-2023	16:19:22	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	28-06-2023	16:19:22	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	28-06-2023	16:19:22	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	28-06-2023	16:19:22	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	28-06-2023	16:19:19	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	28-06-2023	16:19:19	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	28-06-2023	16:19:19	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	28-06-2023	16:19:19	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	28-06-2023	16:19:19	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	28-06-2023	16:19:19	5379	Microsoft-Windows	User Account Manage	N/A	DESKTOP-MD2H
Audit Success	28-06-2023	16:18:43	5059	Microsoft-Windows	Other System Events	N/A	DESKTOP-MD2H
Audit Success	28-06-2023	16:18:43	5061	Microsoft-Windows	System Integrity	N/A	DESKTOP-MD2H

Description

Credential manager credentials were read.

Subject:

Security ID: S-1-5-21-3331464962-214784631-3394824829-1000

Account Name: defaultuser0

Account Domain: DESKTOP-MD2HCPT

Logon ID: 0x20c75

Read Operation: Enumerate Credentials

This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Description Data

Same login ID and details show different

Objects tree

Search

- WIN-BK1Q9542K3L (local)
 - Log Files
 - Microsoft-Windows-Windows Defender%4Operational (C:\Cases\E\Wind
 - System (C:\Cases\E\Windows\System32\winevt\logs\System.evtx)
 - Security (C:\Cases\E\Windows\System32\winevt\logs\Security.evtx)
 - Task templates

Microsoft-Windows-Windows Defender%4Operational.evtx System.evtx Security.evtx

UTC

Type	Date	Time	Event	Source	Category	User	Computer
Audit: Success	3/18/2022	12:24:47 AM	4732	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEdgeWIN10
Audit: Success	3/18/2022	12:24:47 AM	4724	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEdgeWIN10
Audit: Success	3/18/2022	12:24:47 AM	4738	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEdgeWIN10
Audit: Success	3/18/2022	12:24:47 AM	4798	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEdgeWIN10
Audit: Success	3/18/2022	12:24:47 AM	4732	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEdgeWIN10
Audit: Success	3/18/2022	12:24:47 AM	4738	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEdgeWIN10
Audit: Success	3/18/2022	12:24:47 AM	4722	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEdgeWIN10
Audit: Success	3/18/2022	12:24:47 AM	4720	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEdgeWIN10
Audit: Success	3/18/2022	12:24:47 AM	4728	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEdgeWIN10
Audit: Success	3/18/2022	12:10:38 AM	4672	Microsoft-Windows-Security-Auditing	Special Logon	N/A	MSEdgeWIN10
Audit: Success	3/18/2022	12:10:38 AM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	MSEdgeWIN10

Same login ID and details show different

Description

A user account was created.

Subject:

- Security ID: S-1-5-21-3461203602-4096304019-2269080069-1000
- Account Name: IEUser
- Account Domain: MSEdgeWIN10
- Logon ID: 0x452aa

New Account:

- Security ID: S-1-5-21-3461203602-4096304019-2269080069-1003
- Account Name: art-test
- Account Domain: MSEdgeWIN10

Attributes:

- SAM Account Name: art-test
- Display Name: <value not set>
- User Principal Name: -
- Home Directory: <value not set>
- Home Drive: <value not set>
- Script Path: <value not set>
- Profile Path: <value not set>
- User Workstations: <value not set>
- Password Last Set: <never>
- Account Expires: <never>
- Primary Group ID: 513
- Allowed To Delegate To: -
- Old UAC Value: 0x0
- New UAC Value: 0x15
- User Account Control:
 - Account Disabled
 - 'Password Not Required' - Enabled
 - 'Normal Account' - Enabled
- User Parameters: <value not set>
- SID History: -
- Logon Hours: All

Additional Information:

- Privileges: -

Activate Windows
 Go to Settings to activate Windows.

5. Windows Event logs Power shell overview, Analyse Malicious Activity.

Source	Event IDs	Description
Windows PowerShell	400	Engine state is changed from None to Available

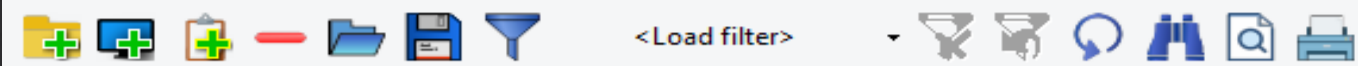
Windows Power shell stored all logs about the command base execution like run the any script , install the any applications , etc.

File Explorer window showing the path: This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > F > Windows > System32 > winevt > logs

Name	Date modified	Type	Size
Microsoft-Windows-VolumeSnapshot-Dr...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-Wcmsvc%4Operatio...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-WebAuthN%4Opera...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-WER-PayloadHealth...	28-06-2023 18:13	Event Log	68 KB
Microsoft-Windows-WFP%4Operational	28-06-2023 16:17	Event Log	68 KB
Microsoft-Windows-Windows Defender...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-Windows Defender...	28-06-2023 16:18	Event Log	68 KB
Microsoft-Windows-Windows Firewall W...	29-06-2023 09:07	Event Log	1,028 KB
Microsoft-Windows-Windows Firewall W...	28-06-2023 16:17	Event Log	68 KB
Microsoft-Windows-WindowsBackup%4...	28-06-2023 16:31	Event Log	68 KB
Microsoft-Windows-WindowsUpdateClie...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-WinINet-Config%4P...	28-06-2023 16:31	Event Log	68 KB
Microsoft-Windows-Winlogon%4Operati...	29-06-2023 09:07	Event Log	1,028 KB
Microsoft-Windows-WinRM%4Operatio...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-WMI-Activity%4Op...	29-06-2023 09:07	Event Log	1,028 KB
Security	29-06-2023 09:07	Event Log	1,092 KB
Setup	28-06-2023 16:17	Event Log	68 KB
System	29-06-2023 09:07	Event Log	1,092 KB
Windows PowerShell	29-06-2023 09:07	Event Log	1,092 KB

101 items | 1 item selected 1.06 MB

Load the windows power shell logs on explorer



Objects tree

- WIN-AJDB7GOIQ
- Log Files
- Task templates

Windows PowerShell.evtx

188 1 UTC

Type	Date	Time	Event	Source	Category	User	Computer
Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	400	PowerShell	Engine Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	28-06-2023	18:02:00	800	PowerShell	Pipeline Execution De	N/A	DESKTOP-MD2H
Information	28-06-2023	18:02:00	800	PowerShell	Pipeline Execution De	N/A	DESKTOP-MD2H
Information	28-06-2023	18:01:44	400	PowerShell	Engine Lifecycle	N/A	DESKTOP-MD2H

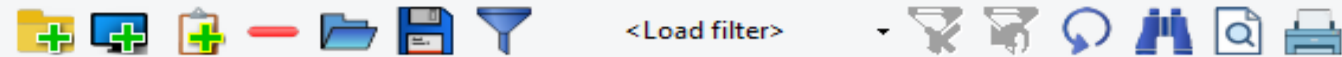
Description

```

HostName=ConsoleHost
HostVersion=5.1.19041.1237
HostId=1cb3bb2b-1850-4cf4-a2b7-0a62cf07c544
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noexit -command Set-Location -literalPath 'C:\Users\Denisha\Desktop\PWF-main\PWF-main\AtomicRed Team'
EngineVersion=5.1.19041.1237
RunspaceId=34b134b3-9b15-4196-839a-39236e79bd83
PipelineId=
CommandName=
CommandType=

```

Description Data



Objects tree

Search

- WIN-AJDB7GOIQ
- Log Files
- Task templates

Windows PowerShell.evtx

188 1 UTC

Type	Date	Time	Event	Source	Category	User	Computer
Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	400	PowerShell	Engine Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
Information	28-06-2023	18:02:00	800	PowerShell	Pipeline Execution De	N/A	DESKTOP-MD2H
Information	28-06-2023	18:02:00	800	PowerShell	Pipeline Execution De	N/A	DESKTOP-MD2H
Information	28-06-2023	18:01:44	400	PowerShell	Engine Lifecycle	N/A	DESKTOP-MD2H

Description

```

UserId=DESKTOP-MD2HCP1\Denisha
HostName=ConsoleHost
HostVersion=5.1.19041.1237
HostId=c8d3a583-872c-4d21-bf69-5e941e11b7d6
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noexit -command Set-Location -literalPath 'C:\Users\Denisha\Desktop\PWF-main\PWF-main\Install-Sysmon'
EngineVersion=5.1.19041.1237
RunspaceId=50a379e5-2c5a-426e-83f6-209ad2331f12
PipelineId=14
ScriptName=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psm1

```

Description Data

Memory Analysis

Setting up volatility3 in Ubuntu

Setting up the Volatility3 in the Ubuntu that open the link <https://bluecapesecurity.com/build-your-forensic-workstation/>

Show the instruction linux based tools.



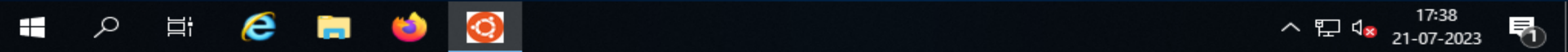
Recycle forensic@WIN-AJDB7GOIQEJ: ~

Try: sudo apt install <deb name>

forensic@WIN-AJDB7GOIQEJ:~\$ sudo apt-get update

```
[sudo] password for forensic:
Get:1 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Hit:2 http://archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:5 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [2304 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal/universe amd64 Packages [8628 kB]
Get:7 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [367 kB]
Get:8 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [13.0 kB]
Get:9 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [1987 kB]
Get:10 http://security.ubuntu.com/ubuntu focal-security/restricted Translation-en [277 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 c-n-f Metadata [576 B]
Get:12 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [858 kB]
Get:13 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [179 kB]
Get:14 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [18.8 kB]
Get:15 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Packages [23.6 kB]
Get:16 http://security.ubuntu.com/ubuntu focal-security/multiverse Translation-en [5504 B]
Get:17 http://archive.ubuntu.com/ubuntu focal/universe Translation-en [5124 kB]
Get:18 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 c-n-f Metadata [548 B]
Get:19 http://archive.ubuntu.com/ubuntu focal/universe amd64 c-n-f Metadata [265 kB]
Get:20 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [144 kB]
Get:21 http://archive.ubuntu.com/ubuntu focal/multiverse Translation-en [104 kB]
Get:22 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 c-n-f Metadata [9136 B]
Get:23 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [2687 kB]
Get:24 http://archive.ubuntu.com/ubuntu focal-updates/main Translation-en [449 kB]
Get:25 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [16.9 kB]
U: Get:26 http://archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [2092 kB]
```

accounts_V... Windows Server 2019 Datacenter Evaluation
Windows License valid for 156 days
Build 17763.rs5_release.180914-1434





```

forensic@WIN-AJDB7GOIQEJ: ~
Fetched 27.7 MB in 22s (1269 kB/s)
Reading package lists... Done
forensic@WIN-AJDB7GOIQEJ:~$ sudo apt install python3-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp cpp-9 dpkg-dev fakeroot g++ g++-9 gcc gcc-9
gcc-9-base libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan5 libatomic1 libbinutils
libc-dev-bin libc6 libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libdpkg-perl libexpat1 libexpat1-dev
libfakeroot libfile-fcntllock-perl libgcc-9-dev libgomp1 libisl22 libitm1 liblsan0 libmpc3 libpython3-dev
libpython3.8 libpython3.8-dev libpython3.8-minimal libpython3.8-stdlib libquadmath0 libstdc++-9-dev libtsan0
libubsan1 linux-libc-dev make manpages-dev python-pip-whl python3-dev python3-wheel python3.8 python3.8-dev
python3.8-minimal zlib1g zlib1g-dev
Suggested packages:
binutils-doc cpp-doc gcc-9-locales debian-keyring g++-multilib g++-9-multilib gcc-9-doc gcc-multilib autoconf
automake libtool flex bison gdb gcc-doc gcc-9-multilib glibc-doc bzip libstdc++-9-doc make-doc python3.8-venv
python3.8-doc binfmt-support
The following NEW packages will be installed:
binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp cpp-9 dpkg-dev fakeroot g++ g++-9 gcc gcc-9
gcc-9-base libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan5 libatomic1 libbinutils
libc-dev-bin libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libdpkg-perl libexpat1-dev libfakeroot
libfile-fcntllock-perl libgcc-9-dev libgomp1 libisl22 libitm1 liblsan0 libmpc3 libpython3-dev libpython3.8-dev
libquadmath0 libstdc++-9-dev libtsan0 libubsan1 linux-libc-dev make manpages-dev python-pip-whl python3-dev
python3-pip python3-wheel python3.8-dev zlib1g-dev
The following packages will be upgraded:
libc6 libexpat1 libpython3.8 libpython3.8-minimal libpython3.8-stdlib python3.8 python3.8-minimal zlib1g
8 upgraded, 50 newly installed, 0 to remove and 251 not upgraded.
Need to get 61.4 MB of archives.
U:After this operation, 228 MB of additional disk space will be used.
accounts_V...

```



forensic@WIN-AJDB7GOIQEJ: ~

update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
Setting up build-essential (12.8ubuntu1.1) ...
Setting up python3-dev (3.8.2-0ubuntu2) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for mime-support (3.64ubuntu1) ...

forensic@WIN-AJDB7GOIQEJ:~\$ pip3

Usage:

pip3 <command> [options]

Commands:

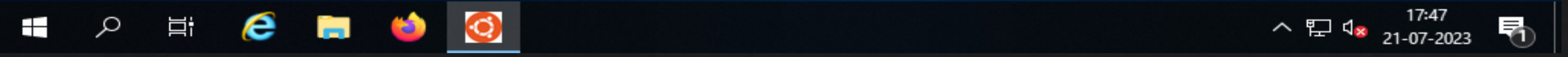
- install Install packages.
- download Download packages.
- uninstall Uninstall packages.
- freeze Output installed packages in requirements format.
- list List installed packages.
- show Show information about installed packages.
- check Verify installed packages have compatible dependencies.
- config Manage local and global configuration.
- search Search PyPI for packages.
- wheel Build wheels from your requirements.
- hash Compute hashes of package archives.
- completion A helper command used for command completion.
- debug Show information useful for debugging.
- help Show help for commands.

General Options:

- h, --help Show help.
- Us --isolated Run pip in an isolated mode, ignoring environment variables and user configuration.

accounts_V...

Windows Server 2019 Datacenter Evaluation
Windows License valid for 156 days
Build 17763.rs5_release.180914-1434





```
forensic@WIN-AJDB7GOIQEJ: ~  
--no-color                Suppress colored output  
--no-python-version-warning Silence deprecation warnings for upcoming unsupported Pythons.  
forensic@WIN-AJDB7GOIQEJ:~$ pip3 install volatility3  
Collecting volatility3  
  Downloading volatility3-2.4.1-py3-none-any.whl (687 kB)  
    |-----| 687 kB 1.0 MB/s  
Collecting pefile>=2017.8.1  
  Downloading pefile-2023.2.7-py3-none-any.whl (71 kB)  
    |-----| 71 kB 4.2 kB/s  
Installing collected packages: pefile, volatility3  
  WARNING: The scripts vol and volshell are installed in '/home/forensic/.local/bin' which is not on PATH.  
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.  
Successfully installed pefile-2023.2.7 volatility3-2.4.1  
forensic@WIN-AJDB7GOIQEJ:~$ pip3 install capstone  
Collecting capstone  
  Downloading capstone-5.0.0.post1-py3-none-manylinux1_x86_64.manylinux2_5_x86_64.whl (2.9 MB)  
    |-----| 2.9 MB 2.1 MB/s  
Installing collected packages: capstone  
Successfully installed capstone-5.0.0.post1  
forensic@WIN-AJDB7GOIQEJ:~$
```

Windows Server 2019 Datacenter Evaluation
Windows License valid for 156 days
Build 17763.rs5_release.180914-1434

forensic@WIN-AJDB7GOIQEJ: ~

forensic@WIN-AJDB7GOIQEJ:~\$ vol -h

Command 'vol' not found, did you mean:

```
command 'gol' from deb growl-for-linux (0.8.5-5)
command 'vl' from deb atfs (1.4pl6-14)
command 'hvol' from deb hfsutils (3.2.6-14)
command 'sol' from deb aisleriot (1:3.22.9-1)
command 'vor' from deb vor (0.5.7-3)
command 'vos' from deb openafs-client (1.8.4~pre1-1ubuntu2.4)
command 'col' from deb bsdmainutils (11.1.2ubuntu3)
```

Try: `sudo apt install <deb name>`

forensic@WIN-AJDB7GOIQEJ:~\$ ls -la

```
total 8
drwxr-xr-x 1 forensic forensic 512 Jul 21 17:48 .
drwxr-xr-x 1 root      root      512 Jun 28 05:44 ..
-rw----- 1 forensic forensic 140 Jul 16 06:27 .bash_history
-rw-r--r-- 1 forensic forensic 220 Jun 28 05:44 .bash_logout
-rw-r--r-- 1 forensic forensic 3771 Jun 28 05:44 .bashrc
drwxrwxrwx 1 forensic forensic 512 Jul 21 17:48 .cache
drwxr-xr-x 1 forensic forensic 512 Jun 28 05:45 .landscape
drwx----- 1 forensic forensic 512 Jul 21 17:48 .local
-rw-rw-rw- 1 forensic forensic  0 Jul 21 17:32 .motd_shown
-rw-r--r-- 1 forensic forensic 807 Jun 28 05:44 .profile
-rw-r--r-- 1 forensic forensic  0 Jul 21 17:37 .sudo_as_admin_successful
```

forensic@WIN-AJDB7GOIQEJ:~\$ source .profile

forensic@WIN-AJDB7GOIQEJ:~\$ vol -h

Volatility 3 Framework 2.4.1

```
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS]
                 [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config]
                 [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline]
                 [--single-location SINGLE_LOCATION] [--stackers [STACKERS [STACKERS ...]]]
                 [--single-swap-locations [SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_LOCATIONS ...]]]
                 plugin ...
```



17:51

21-07-2023



1

What is memory Analysis

Memory forensics (sometimes referred to as memory analysis) refers to the analysis of volatile data in a computer's memory dump. Information security professionals conduct memory forensics to investigate and identify attacks or malicious behaviors that do not leave easily detectable tracks on hard drive data.

Copy the target machine memory image from host system and paste the memory in cases > Analysis > memory folder create > paste Here.

Open the Ubuntu linux. Go to the path on memory image file did paste.

```
forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/Memory
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

System information as of Sat Jul 22 07:54:56 DST 2023

System load: 0.52      Processes: 7
Usage of /home: unknown  Users logged in: 0
Memory usage: 43%      IPv4 address for eth0: 10.0.2.15
Swap usage: 1%

259 updates can be applied immediately.
188 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

This message is shown once a day. To disable it please create the
/home/forensic/.hushlogin file.
forensic@WIN-AJDB7GOIQEJ:~$ pwd
/home/forensic
forensic@WIN-AJDB7GOIQEJ:~$ cd /mnt
forensic@WIN-AJDB7GOIQEJ:/mnt$ ls
.
forensic@WIN-AJDB7GOIQEJ:/mnt$ cd ..
forensic@WIN-AJDB7GOIQEJ:/$ ls
bin  dev  home  lib  lib64  media  opt  root  sbin  srv  tmp  var
boot  etc  init  lib32  libx32  mnt  proc  run  snap  sys  usr
forensic@WIN-AJDB7GOIQEJ:/$ cd /mnt/c/Cases/Analysis/Memory/
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ pwd
/mnt/c/Cases/Analysis/Memory
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ ls -la
total 2234248
drwxrwxrwx 1 forensic forensic 512 Jul 22 07:49 .
drwxrwxrwx 1 forensic forensic 512 Jul 22 07:49 ..
-rwxrwxrwx 1 forensic forensic 2287868348 Jul 22 06:38 win10-memory.raw
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$
```

Gathering Windows system information with Volatility3

```
Select forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/Memory
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -h
Volatility 3 Framework 2.4.1
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS]
                [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG]
                [--clear-cache] [--cache-path CACHE_PATH] [--offline] [--single-location SINGLE_LOCATION]
                [--stackers [STACKERS [STACKERS ...]]]
                [--single-swap-locations [SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_LOCATIONS ...]]]
                plugin ...

An open-source memory forensics framework

optional arguments:
  -h, --help                Show this help message and exit, for specific plugin options use 'volatility <pluginname> --help'
  -c CONFIG, --config CONFIG
                           Load the configuration from a json file
  --parallelism [{processes,threads,off}]
                           Enables parallelism (defaults to off if no argument given)
  -e EXTEND, --extend EXTEND
                           Extend the configuration with a new (or changed) setting
  -p PLUGIN_DIRS, --plugin-dirs PLUGIN_DIRS
                           Semi-colon separated list of paths to find plugins
  -s SYMBOL_DIRS, --symbol-dirs SYMBOL_DIRS
                           Semi-colon separated list of paths to find symbols
  -v, --verbosity           Increase output verbosity
  -l LOG, --log LOG        Log output to a file as well as the console
  -o OUTPUT_DIR, --output-dir OUTPUT_DIR
                           Directory in which to output any generated files
  -q, --quiet              Remove progress feedback
  -r RENDERER, --renderer RENDERER
                           Determines how to render the output (quick, none, csv, pretty, json, jsonl)
  -f FILE, --file FILE     Shorthand for --single-location=file:// if single-location is not defined
  --write-config           Write configuration JSON file out to config.json
  --save-config SAVE_CONFIG
                           Save configuration JSON file to a file
  --clear-cache           Clears out all short-term cached items
  --cache-path CACHE_PATH
                           Change the default path (/home/forensic/.cache/volatility3) used to store the cache
```

Type the command for volatility help and show all plugins for different operating system.

```
Checks for malicious trustedbsd modules
mac.vfsevents.VFSEvents
Lists processes that are filtering file system events
timeliner.Timeliner
Runs all relevant plugins that provide time related information and orders the results by time.
windows.bigpools.BigPools
List big page pools.
windows.callbacks.Callbacks
Lists kernel callbacks and notification routines.
windows.cmdline.CmdLine
Lists process command line arguments.
windows.crashinfo.Crashinfo
windows.devicetree.DeviceTree
Listing tree based on drivers and attached devices in a particular windows memory image.
windows.dlllist.DllList
Lists the loaded modules in a particular windows memory image.
windows.driverirp.DriverIrp
List IRPs for drivers in a particular windows memory image.
windows.drivermodule.DriverModule
Determines if any loaded drivers were hidden by a rootkit
windows.driverscan.DriverScan
Scans for drivers present in a particular windows memory image.
windows.dumpfiles.DumpFiles
Dumps cached file contents from Windows memory samples.
windows.envvars.Envvars
Display process environment variables
windows.filescan.FileScan
Scans for file objects present in a particular windows memory image.
windows.getservicesids.GetServiceSIDs
Lists process token sids.
windows.getsids.GetSIDs
Print the SIDs owning each process
windows.handles.Handles
Lists process open handles.
windows.info.Info Show OS & kernel details of the memory sample being analyzed.
windows.joblinks.JobLinks
Print process job link information
```

we have use
windows info
plugins .



08:12

22-07-2023



1

```

Progress: 99.98      Reading Symbol layer
Progress: 99.98      Reading Symbol layer
Progress: 99.99      Reading Symbol layer
Progress: 99.99      Reading Symbol layer
Progress: 99.99      Reading Symbol layer
Progress: 99.99      Reading Symbol layer
Progress: 99.99      Reading Symbol layer
Progress: 99.99      Reading Symbol layer
Progress: 99.99      Reading Symbol layer
Progress: 100.00     Reading Symbol layer
Progress: 100.00     Reading Symbol layer
Progress: 100.00     PDB scanning finished

```

```

Variable      Value
Kernel Base   0xf8063d41d000
DTB           0x1aa000
Symbols file:///home/forensic/.local/lib/python3.8/site-packages/volatility3/symbols/windows/ntkrnlmp.pdb/CA8E2F01B822EDE6357
898BFBF862997-1.json.xz
Is64Bit       True
IsPAE         False
layer_name    0 WindowsIntel32e
memory_layer  1 Elf64Layer
base_layer    2 FileLayer
KdVersionBlock 0xf8063e02c368
Major/Minor   15.19041
MachineType   34404
KeNumberProcessors 2
SystemTime    2023-07-22 06:37:29
NtSystemRoot  C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 10
NtMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine     34404
PE TimeDateStamp Wed Jan 4 04:27:11 1995

```

← Type this command how the result.

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.info
```

```
memory_layer 1 Elf64Layer
base_layer 2 FileLayer
KdVersionBlock 0xf8063e02c368
Major/Minor 15.19041
MachineType 34404
KeNumberProcessors 2
SystemTime 2023-07-22 06:37:29
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 10
NtMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine 34404
```

Using the pstree plugin list out the how many services are running.

```
PE TimeDateStamp Wed Jan 4 04:27:11 1995
```

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pstree
```

```
Volatility 3 Framework 2.4.1
```

```
^Z^Cress: 11.38 Scanning memory_layer using BytesScanner
```

```
[1]+ Stopped vol -f win10-memory.raw windows.pstree
```

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pstree > pstree.txt
```

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pstree
```

```
Volatility 3 Framework 2.4.1
```

```
Progress: 100.00
```

```
PDB scanning finished
```

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime
4	0	System	0xcc068767d080	124	-	N/A	False	2023-07-22 06:33:09.000000	N/A
* 1404	4	MemCompression	0xcc068e308040	14	-	N/A	False	2023-07-22 06:34:20.000000	N/A
* 92	4	Registry	0xcc06877b6040	4	-	N/A	False	2023-07-22 06:30:52.000000	N/A
* 348	4	smss.exe	0xcc0687c6c040	2	-	N/A	False	2023-07-22 06:33:09.000000	N/A
532	512	csrss.exe	0xcc068d369080	12	-	1	False	2023-07-22 06:33:37.000000	N/A
596	512	winlogon.exe	0xcc068a750240	6	-	1	False	2023-07-22 06:33:37.000000	N/A
* 800	596	fontdrvhost.ex	0xcc068d3f6080	5	-	1	False	2023-07-22 06:33:40.000000	N/A
* 2180	596	userinit.exe	0xcc068eaaf080	0	-	1	False	2023-07-22 06:36:41.000000	2023-07-22 06:36:56.000000
** 2488	2180	explorer.exe	0xcc068ec78080	49	-	1	False	2023-07-22 06:36:43.000000	N/A
* 976	596	dwm.exe	0xcc068e14a300	16	-	1	False	2023-07-22 06:33:42.000000	N/A

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$
```



08:48

22-07-2023



1

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pslist -h
```

Volatility 3 Framework 2.4.1

```
usage: volatility windows.pslist.PsList [-h] [--physical] [--pid [PID [PID ...]]] [--dump]
```

optional arguments:

- h, --help show this help message and exit
- physical Display physical offsets instead of virtual
- pid [PID [PID ...]] Process ID to include (all other processes are excluded)
- dump Extract listed processes

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pslist 596
```

Volatility 3 Framework 2.4.1

```
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline] [--single-location SINGLE_LOCATION] [--stackers [STACKERS [STACKERS ...]]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_LOCATIONS ...]]] plugin ...
```

volatility: error: unrecognized arguments: 596

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pslist 0596
```

Volatility 3 Framework 2.4.1

```
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline] [--single-location SINGLE_LOCATION] [--stackers [STACKERS [STACKERS ...]]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_LOCATIONS ...]]] plugin ...
```

volatility: error: unrecognized arguments: 0596

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pslist 0596
```

Volatility 3 Framework 2.4.1

```
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline] [--single-location SINGLE_LOCATION] [--stackers [STACKERS [STACKERS ...]]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_LOCATIONS ...]]] plugin ...
```

volatility: error: unrecognized arguments: 0596

Using pslist plugin gather information using pid.

```
 [--stackers [STACKERS [STACKERS ...]]]
 [--single-swap-locations [SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_LOCATIONS ...]]]
 plugin ...
```

volatility: error: unrecognized arguments: 596

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pslist 0596
```

Volatility 3 Framework 2.4.1

```
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS]
 [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG]
 [--clear-cache] [--cache-path CACHE_PATH] [--offline] [--single-location SINGLE_LOCATION]
 [--stackers [STACKERS [STACKERS ...]]]
 [--single-swap-locations [SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_LOCATIONS ...]]]
 plugin ...
```

volatility: error: unrecognized arguments: 0596

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pslist 0596
```

Volatility 3 Framework 2.4.1

```
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS]
 [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG]
 [--clear-cache] [--cache-path CACHE_PATH] [--offline] [--single-location SINGLE_LOCATION]
 [--stackers [STACKERS [STACKERS ...]]]
 [--single-swap-locations [SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_LOCATIONS ...]]]
 plugin ...
```

volatility: error: unrecognized arguments: 0596

Show the services for individual pid

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$
```

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$
```

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pslist --pid 596
```

Volatility 3 Framework 2.4.1

Progress: 100.00 PDB scanning finished

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File
596	512	winlogon.exe	0xcc068a750240	6	-	1	False	2023-07-22 06:33:37.000000	N/A	Disabled

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$
```

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$
```

```
forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/Memory
* 92      4      Registry      0xcc06877b6040 4      -      N/A      False      2023-07-22 06:30:52.000000      N/A
* 348     4      smss.exe      0xcc0687c6c040 2      -      N/A      False      2023-07-22 06:33:09.000000      N/A
532      512     csrss.exe     0xcc068d369080 12     -      1        False      2023-07-22 06:33:37.000000      N/A
596      512     winlogon.exe  0xcc068a750240 6      -      1        False      2023-07-22 06:33:37.000000      N/A
* 800     596     fontdrvhost.ex 0xcc068d3f6080 5      -      1        False      2023-07-22 06:33:40.000000      N/A
* 2180    596     userinit.exe  0xcc068eaaf080 0      -      1        False      2023-07-22 06:36:41.000000      2023-07-22 06
:36:56.000000
** 2488   2180    explorer.exe   0xcc068ec78080 49     -      1        False      2023-07-22 06:36:43.000000      N/A
* 976     596     dwm.exe       0xcc068e14a300 16     -      1        False      2023-07-22 06:33:42.000000      N/A
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.dlllist --pid 596
Volatility 3 Framework 2.4.1
^CTraceback (most recent call last):
  File "/home/forensic/.local/bin/vol", line 8, in <module>
    sys.exit(main())
  File "/home/forensic/.local/lib/python3.8/site-packages/volatility3/cli/__init__.py", line 797, in main
    CommandLine().run()
  File "/home/forensic/.local/lib/python3.8/site-packages/volatility3/cli/__init__.py", line 302, in run
    automagics = automagic.available(ctx)
  File "/home/forensic/.local/lib/python3.8/site-packages/volatility3/framework/automagic/__init__.py", line 37, in available
    import_files(sys.modules[__name__])
  File "/home/forensic/.local/lib/python3.8/site-packages/volatility3/framework/__init__.py", line 152, in import_files
    failures += import_file(
  File "/home/forensic/.local/lib/python3.8/site-packages/volatility3/framework/__init__.py", line 184, in import_file
    importlib.import_module(module)
  File "/usr/lib/python3.8/importlib/__init__.py", line 127, in import_module
    return _bootstrap._gcd_import(name[level:], package, level)
  File "<frozen importlib._bootstrap>", line 1014, in _gcd_import
  File "<frozen importlib._bootstrap>", line 991, in _find_and_load
  File "<frozen importlib._bootstrap>", line 975, in _find_and_load_unlocked
  File "<frozen importlib._bootstrap>", line 671, in _load_unlocked
  File "<frozen importlib._bootstrap_external>", line 844, in exec_module
  File "<frozen importlib._bootstrap_external>", line 939, in get_code
  File "<frozen importlib._bootstrap_external>", line 1038, in get_data
KeyboardInterrupt

forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.dlllist --pid 596 > dll.txt
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$
```

Search other files run on pid no 596 using dll list.

File Home Share View

Pin to Quick access Copy Paste Cut Copy path Paste shortcut

Clipboard

← → ↕ This PC > SDT_x64FRE

- Evidence
- Execution
- Memory
- Registry
- This PC
- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- SDT_x64FRE_EN
- CD Drive (D:) Vir
- Downloads (\\V
- Network

3 items 1 item selected 5.66 KB

File Edit Format View Help

utility 3 Framework 2.4.1

Process	Base	Size	Name	Path	LoadTime	File output
winlogon.exe	0x7ff674bb0000			0xec000	winlogon.exe	C:\Windows\system32\winlogon.ex
winlogon.exe	0x7ff942430000			0x1f5000	ntdll.dll	C:\Windows\SYSTEM32\ntc
winlogon.exe	0x7ff941f10000			0xbe000	KERNEL32.DLL	C:\Windows\System32\KERNEL32.DL
winlogon.exe	0x7ff93fe70000			0x2c9000	KERNELBASE.dll	C:\Windows\System32\KEF
winlogon.exe	0x7ff941e70000			0x9e000	msvcrt.dll	C:\Windows\System32\msvcrt.dll
winlogon.exe	0x7ff942350000			0x9b000	sechost.dll	C:\Windows\System32\sechost.dll
winlogon.exe	0x7ff941480000			0x12a000	RPCRT4.dll	C:\Windows\System32\RPC
winlogon.exe	0x7ff940630000			0x355000	combase.dll	C:\Windows\System32\con
winlogon.exe	0x7ff940210000			0x100000	ucrtbase.dll	C:\Windows\System32\ucr
winlogon.exe	0x7ff9412f0000			0xac000	advapi32.dll	C:\Windows\System32\advapi32.dl
winlogon.exe	0x7ff93f9c0000			0x4b000	powrprof.dll	C:\Windows\SYSTEM32\powrprof.dl
winlogon.exe	0x7ff93f9a0000			0x12000	UMPDC.dll	C:\Windows\system32\UMPDC.dll
winlogon.exe	0x7ff93fa90000			0x1f000	profapi.dll	C:\Windows\system32\profapi.dll
winlogon.exe	0x7ff940480000			0x1a1000	user32.dll	C:\Windows\System32\use
winlogon.exe	0x7ff93fb50000			0x22000	win32u.dll	C:\Windows\System32\win32u.dll
winlogon.exe	0x7ff9417b0000			0x2b000	GDI32.dll	C:\Windows\System32\GDI32.dll
winlogon.exe	0x7ff940310000			0x10b000	gdi32full.dll	C:\Windows\System32\gdi
winlogon.exe	0x7ff940140000			0x9d000	msvcp_win.dll	C:\Windows\System32\msvcp_win.c
winlogon.exe	0x7ff942290000			0x30000	IMM32.DLL	C:\Windows\System32\IMM32.DLL
winlogon.exe	0x7ff93f890000			0x5a000	winsta.dll	C:\Windows\SYSTEM32\winsta.dll

Unix (LF) Ln 1, Col 1 100%

All dll file here.

KeyboardInterrupt

```
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.dlllist --pid 596 > dll.txt
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.dlllist --pid 596 --dump
```

Volatility 3 Framework 2.4.1

Progress: 100.00

PDB scanning finished

Extract the files and give more information

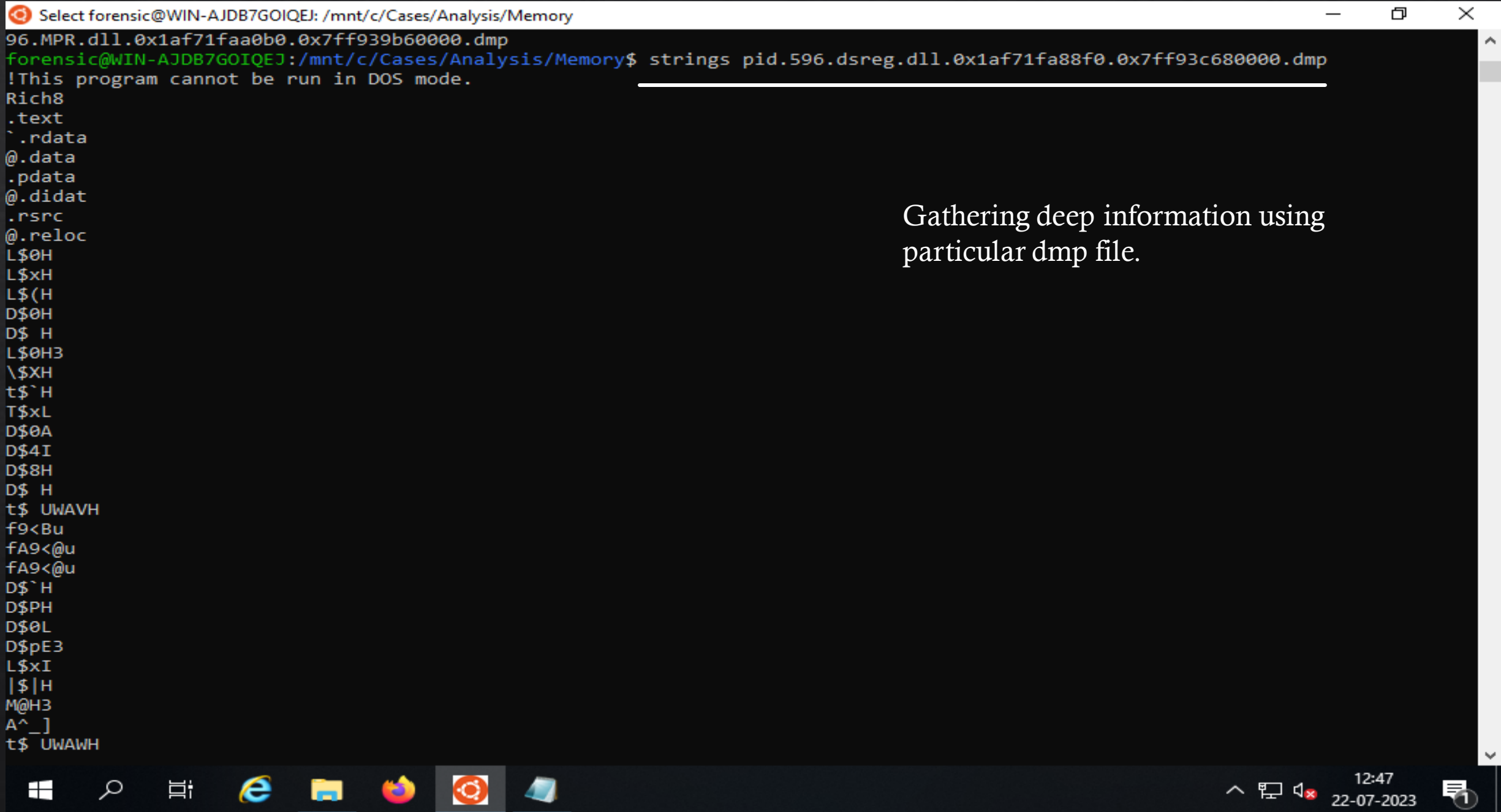
PID	Process	Base	Size	Name	Path	LoadTime	File output
596	winlogon.exe	0x7ff674bb0000	0xec000	winlogon.exe	C:\Windows\system32\winlogon.exe	2023-07-22 06:33:37.0	
00000	pid.596.winlogon.exe.0x1af71f81e90.0x7ff674bb0000.dmp						
596	winlogon.exe	0x7ff942430000	0x1f5000	ntdll.dll	C:\Windows\SYSTEM32\ntdll.dll	2023-07-22 06:33:37.0	
00000	pid.596.ntdll.dll.0x1af71f81d00.0x7ff942430000.dmp						
596	winlogon.exe	0x7ff941f10000	0xbe000	KERNEL32.DLL	C:\Windows\System32\KERNEL32.DLL	2023-07-22 06:33:37.0	
00000	pid.596.KERNEL32.DLL.0x1af71f82430.0x7ff941f10000.dmp						
596	winlogon.exe	0x7ff93fe70000	0x2c9000	KERNELBASE.dll	C:\Windows\System32\KERNELBASE.dll	2023-07-22 06:33:37.000000	
00000	pid.596.KERNELBASE.dll.0x1af71f82a40.0x7ff93fe70000.dmp						
596	winlogon.exe	0x7ff941e70000	0x9e000	msvcrt.dll	C:\Windows\System32\msvcrt.dll	2023-07-22 06:33:37.000000	p
id.596.msvcrt.dll.0x1af71f83c50.0x7ff941e70000.dmp							
596	winlogon.exe	0x7ff942350000	0x9b000	sechost.dll	C:\Windows\System32\sechost.dll	2023-07-22 06:33:37.000000	p
id.596.sechost.dll.0x1af71f83fd0.0x7ff942350000.dmp							
596	winlogon.exe	0x7ff941480000	0x12a000	RPCRT4.dll	C:\Windows\System32\RPCRT4.dll	2023-07-22 06:33:37.0	
00000	pid.596.RPCRT4.dll.0x1af71f843c0.0x7ff941480000.dmp						
596	winlogon.exe	0x7ff940630000	0x355000	combase.dll	C:\Windows\System32\combase.dll	2023-07-22 06:33:37.0	
00000	pid.596.combase.dll.0x1af71f84800.0x7ff940630000.dmp						
596	winlogon.exe	0x7ff940210000	0x100000	ucrtbase.dll	C:\Windows\System32\ucrtbase.dll	2023-07-22 06:33:37.000000	
id.596.ucrtbase.dll.0x1af71f84cc0.0x7ff940210000.dmp							
596	winlogon.exe	0x7ff9412f0000	0xac000	advapi32.dll	C:\Windows\System32\advapi32.dll	2023-07-22 06:33:37.0	
00000	pid.596.advapi32.dll.0x1af71f85680.0x7ff9412f0000.dmp						
596	winlogon.exe	0x7ff93f9c0000	0x4b000	powrprof.dll	C:\Windows\SYSTEM32\powrprof.dll	2023-07-22 06:33:37.0	
00000	pid.596.powrprof.dll.0x1af71f850e0.0x7ff93f9c0000.dmp						
596	winlogon.exe	0x7ff93f9a0000	0x12000	UMPDC.dll	C:\Windows\system32\UMPDC.dll	2023-07-22 06:33:37.000000	p
id.596.UMPDC.dll.0x1af71f91ac0.0x7ff93f9a0000.dmp							
596	winlogon.exe	0x7ff93fa90000	0x1f000	profapi.dll	C:\Windows\system32\profapi.dll	2023-07-22 06:33:37.000000	p
id.596.profapi.dll.0x1af71f849e0.0x7ff93fa90000.dmp							
596	winlogon.exe	0x7ff940480000	0x1a1000	user32.dll	C:\Windows\System32\user32.dll	2023-07-22 06:33:37.0	
00000	pid.596.user32.dll.0x1af71f96e90.0x7ff940480000.dmp						
596	winlogon.exe	0x7ff93fb50000	0x22000	win32u.dll	C:\Windows\System32\win32u.dll	2023-07-22 06:33:37.000000	p

File Explorer window showing the contents of the Memory folder. The address bar indicates the path: This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > Analysis > Memory. The left sidebar shows the folder structure, with SDT_x64FREE_EN selected. The main pane displays a list of files, including a Text Document named 'dll' and several DMP Files.

Name	Date modified	Type	Size
dll	22-07-2023 12:36	Text Document	6 KB
pid.596.advapi32.dll.0x1af71f85680.0x7ff9...	22-07-2023 12:44	DMP File	688 KB
pid.596.apphelp.dll.0x1af71fa9ac0.0x7ff93...	22-07-2023 12:45	DMP File	576 KB
pid.596.Bcrypt.dll.0x1af71f98d70.0x7ff940...	22-07-2023 12:44	DMP File	156 KB
pid.596.bcryptprimitives.dll.0x1af71f98ea...	22-07-2023 12:44	DMP File	524 KB
pid.596.combase.dll.0x1af71f84800.0x7ff9...	22-07-2023 12:44	DMP File	3,412 KB
pid.596.CRYPT32.dll.0x1af71fa9860.0x7ff9...	22-07-2023 12:45	DMP File	1,368 KB
pid.596.CRYPTBASE.dll.0x1af71fa8db0.0x...	22-07-2023 12:45	DMP File	48 KB
pid.596.cryptsp.dll.0x1af71fa87c0.0x7ff93f...	22-07-2023 12:45	DMP File	96 KB
pid.596.DNSAPI.dll.0x1af71f98780.0x7ff93...	22-07-2023 12:44	DMP File	816 KB
pid.596.DPAPI.dll.0x1af71fa9990.0x7ff93f8...	22-07-2023 12:45	DMP File	40 KB
pid.596.dsreg.dll.0x1af71fa88f0.0x7ff93c6...	22-07-2023 12:45	DMP File	1,276 KB
pid.596.dwmapi.dll.0x1af71fa94d0.0x7ff93...	22-07-2023 12:45	DMP File	188 KB
pid.596.dwminit.dll.0x1af71fa9600.0x7ff93...	22-07-2023 12:45	DMP File	80 KB
pid.596.firewallapi.dll.0x1af71f99100.0x7ff...	22-07-2023 12:44	DMP File	636 KB
pid.596.fwbases.dll.0x1af71fa8430.0x7ff93e...	22-07-2023 12:44	DMP File	188 KB
pid.596.GDI32.dll.0x1af71f98270.0x7ff9417...	22-07-2023 12:44	DMP File	172 KB
pid.596.gdi32full.dll.0x1af71f988b0.0x7ff9...	22-07-2023 12:44	DMP File	1,068 KB
pid.596.IMM32.DLL.0x1af71f983f0.0x7ff94...	22-07-2023 12:44	DMP File	192 KB

Show the all dump file in memory folder

50 items | 1 item selected 5.66 KB



Select forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/Memory

96.MPR.dll.0x1af71faa0b0.0x7ff939b60000.dmp

forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory\$ strings pid.596.dsreg.dll.0x1af71fa88f0.0x7ff93c680000.dmp

!This program cannot be run in DOS mode.

Rich8

.text

^.rdata

@.data

.pdata

@.didat

.rsrc

@.reloc

L\$0H

L\$xH

L\$(H

D\$0H

D\$ H

L\$0H3

\\$XH

t\$`H

T\$xL

D\$0A

D\$4I

D\$8H

D\$ H

t\$ UWAVH

f9<Bu

fA9<@u

fA9<@u

D\$`H

D\$PH

D\$0L

D\$pE3

L\$xI

|\$|H

M@H3

A^_]

t\$ UWAWH

Gathering deep information using particular dmp file.



12:47
22-07-2023



Identify process owners and associated SIDs

Windows.getsids.GetSIDs plugin use for print SIDs owning each process.

```
forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/Memory
TTBL
TEMP
TEMPPP
H7^A
TEMP$
TEMP
TEMP
TEMP
TEMPd
ivO1
TEMP
g=z=
TEMP
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.getsids -h
Volatility 3 Framework 2.4.1
usage: volatility windows.getsids.GetSIDs [-h] [--pid [PID [PID ...]]]

optional arguments:
  -h, --help            show this help message and exit
  --pid [PID [PID ...]]
                        Filter on specific process IDs

forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.getsids --pid 596 532
Volatility 3 Framework 2.4.1
Progress: 100.00          PDB scanning finished
PID      Process SID          Name
532      csrss.exe             S-1-5-18              Local System
532      csrss.exe             S-1-5-32-544          Administrators
532      csrss.exe             S-1-1-0               Everyone
532      csrss.exe             S-1-5-11              Authenticated Users
532      csrss.exe             S-1-16-16384          System Mandatory Level
596      winlogon.exe          S-1-5-18              Local System
596      winlogon.exe          S-1-5-32-544          Administrators
596      winlogon.exe          S-1-1-0               Everyone
596      winlogon.exe          S-1-5-11              Authenticated Users
596      winlogon.exe          S-1-16-16384          System Mandatory Level
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$
```

Getsids plugin use for find the owner of the process show the output here.

Detecting and Analyzing malicious registry key entries from memory

```
forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/Memory
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.registry.printkey -h
Volatility 3 Framework 2.4.1
usage: volatility windows.registry.printkey.PrintKey [-h] [--offset OFFSET] [--key KEY] [--recurse]

optional arguments:
  -h, --help            show this help message and exit
  --offset OFFSET       Hive Offset
  --key KEY             Key to start from
  --recurse            Recurses through keys
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.registry.hivelist
Volatility 3 Framework 2.4.1
Progress: 100.00          PDB scanning finished
Offset  FileFullPath          File output
0xa3030e855000          Disabled
0xa3030e898000          \REGISTRY\MACHINE\SYSTEM          Disabled
0xa3030e8f1000          \REGISTRY\MACHINE\HARDWARE        Disabled
0xa303105e5000          \SystemRoot\System32\Config\SAM    Disabled
0xa30310551000          \SystemRoot\System32\Config\SECURITY Disabled
0xa303105f1000          \SystemRoot\System32\Config\DEFAULT Disabled
0xa303105e7000          \SystemRoot\System32\Config\SOFTWARE Disabled
0xa303124b0000          \Device\HarddiskVolume1\Boot\BCD   Disabled
0xa3031282b000          \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT          Disabled
0xa30312a47000          \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT          Disabled
0xa30312a3e000          \SystemRoot\System32\Config\BBI     Disabled
0xa30313e2c000          \??\C:\Windows\AppCompat\Programs\Amcache.hve          Disabled
0xa30314219000          \??\C:\Users\Denisha\ntuser.dat     Disabled
0xa30314774000          \??\C:\Users\Denisha\AppData\Local\Microsoft\Windows\UsrClass.dat          Disabled
0xa30316deb000          \SystemRoot\System32\config\DRIVERS Disabled
0xa30317618000          \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Search_1.14.2.19041_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat Disabled
0xa30317586000          \??\C:\Users\Denisha\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\Settings\settings.dat Disabled
0xa303177b6000          \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.StartMenuExperienceHost_10.0.19041.1023_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat Disabled
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.registry.printkey --offset 0xa30314774000 --key AtomicRedTeam
```

Using registry print key and registry hive list find information specific key value.



13:26
22-07-2023



1

```
forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/Memory
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.registry.printkey --offset 0xa30314774
000 --key AtomicRedTeam
```

Using this command find the detail about Atomic RedTeam key value(any key enter).



13:33
22-07-2023



Super Timeline Analysis

A detailed timeline of everything that occurred on a system, also known as a Super Timeline, can be extremely beneficial in determining what took place in a digital investigation.

1. Prepare Tools

- Volatility3
- Plaso Log2Timeline
- QEMU

2. Prepare Evidence

- Disk image(RAW!)
- Memory image

3. Run Tools

- Memory-generate bodyfile
- Disk-generate plaso file
- Merge files
- Generate super timeline with psort

4. Timeline Analysis

- EZ Timeline Explorer

Prepare tools and Converting the disk image with QEMU

Use the link for install the Tools

```
forensic@WIN-AJDB7GOIQEJ: ~  
forensic@WIN-AJDB7GOIQEJ:~$ sudo add-apt-repository ppa:gift/stable  
[sudo] password for forensic:  
Periodic releases, contains periodic releases intended for non-development use  
More info: https://launchpad.net/~gift/+archive/ubuntu/stable  
Press [ENTER] to continue or Ctrl-c to cancel adding it.  
  
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease  
Hit:2 http://archive.ubuntu.com/ubuntu focal-updates InRelease  
Hit:3 http://security.ubuntu.com/ubuntu focal-security InRelease  
Get:4 http://ppa.launchpad.net/gift/stable/ubuntu focal InRelease [18.0 kB]  
Hit:5 http://archive.ubuntu.com/ubuntu focal-backports InRelease  
  
-
```

Add the plaso GIFT repository for this command.

forensic@WIN-AJDB7GOIQEJ: ~

Get:4 http://ppa.launchpad.net/gift/stable/ubuntu focal InRelease [18.0 kB]

Hit:5 http://archive.ubuntu.com/ubuntu focal-backports InRelease

0% [Working]

Get:6 http://ppa.launchpad.net/gift/stable/ubuntu focal/main amd64 Packages [63.0 kB]

Get:7 http://ppa.launchpad.net/gift/stable/ubuntu focal/main Translation-en [17.1 kB]

Fetched 98.1 kB in 6min 19s (258 B/s)

Reading package lists... Done

forensic@WIN-AJDB7GOIQEJ:~\$

forensic@WIN-AJDB7GOIQEJ:~\$ sudo apt install qemu-utils

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following additional packages will be installed:

ibverbs-providers libboost-iostreams1.71.0 libboost-thread1.71.0 libibverbs1 libiscsi7 libnl-3-200 libnl-route-3-200
librados2 librbd1 librdmacm1 qemu-block-extra sharutils

Suggested packages:

debootstrap sharutils-doc bsd-mailx | mailx

The following NEW packages will be installed:

ibverbs-providers libboost-iostreams1.71.0 libboost-thread1.71.0 libibverbs1 libiscsi7 libnl-3-200 libnl-route-3-200
librados2 librbd1 librdmacm1 qemu-block-extra qemu-utils sharutils

0 upgraded, 13 newly installed, 0 to remove and 261 not upgraded.

Need to get 7133 kB of archives.

After this operation, 33.7 MB of additional disk space will be used.

Do you want to continue? [Y/n] Y

Get:1 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 libnl-3-200 amd64 3.4.0-1ubuntu0.1 [54.4 kB]

Get:2 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 libnl-route-3-200 amd64 3.4.0-1ubuntu0.1 [151 kB]

Get:3 http://archive.ubuntu.com/ubuntu focal/main amd64 libibverbs1 amd64 28.0-1ubuntu1 [53.6 kB]

Get:4 http://archive.ubuntu.com/ubuntu focal/main amd64 ibverbs-providers amd64 28.0-1ubuntu1 [232 kB]

Get:5 http://archive.ubuntu.com/ubuntu focal/main amd64 libboost-iostreams1.71.0 amd64 1.71.0-6ubuntu6 [237 kB]

Get:6 http://archive.ubuntu.com/ubuntu focal/main amd64 libboost-thread1.71.0 amd64 1.71.0-6ubuntu6 [249 kB]

Get:7 http://archive.ubuntu.com/ubuntu focal/main amd64 librdmacm1 amd64 28.0-1ubuntu1 [64.9 kB]

Get:8 http://archive.ubuntu.com/ubuntu focal/main amd64 libiscsi7 amd64 1.18.0-2 [63.9 kB]

Get:9 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 librados2 amd64 15.2.17-0ubuntu0.20.04.4 [3227 kB]

Get:10 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 librbd1 amd64 15.2.17-0ubuntu0.20.04.4 [1625 kB]

Get:11 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 qemu-block-extra amd64 1:4.2-3ubuntu6.27 [53.4 kB]

Get:12 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 qemu-utils amd64 1:4.2-3ubuntu6.27 [969 kB]

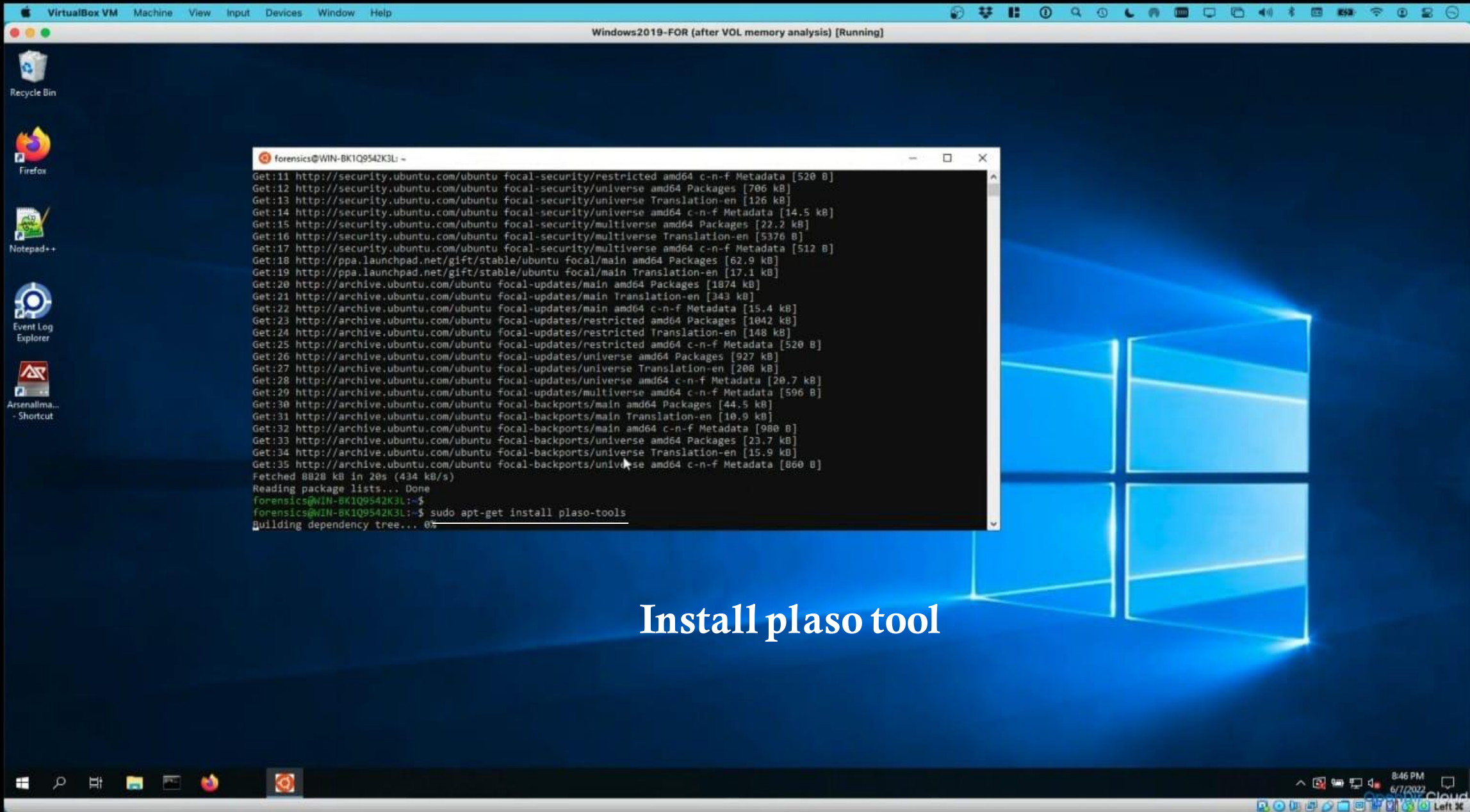
87% [12 qemu-utils 273 kB/969 kB 28%]

1010 kB/s 0s



06:23
24-07-2023





Install plaso tool

File Explorer window showing the path: This PC > Downloads (\\VBoxSvr) (Z:) > Evidence. The ribbon includes File, Home, Share, View, Manage, and Disc Image Tools. The ribbon buttons are: Pin to Quick access, Copy, Paste, Cut, Copy path, Paste shortcut, Move to, Copy to, Delete, Rename, New folder, New item, Easy access, Properties, Open, Edit, Select all, Select none, and Invert selection.

The address bar shows: > This PC > Downloads (\\VBoxSvr) (Z:) > Evidence

The left sidebar shows the following items: Evidence, Execution, NTFS, Registry, This PC, 3D Objects, Desktop, Documents, Downloads, Music, Pictures, Videos, SDT_x64FREE_EN, CD Drive (D:) Vir, Downloads (\\V, and Network.

Name	Date modified	Type	Size
 {0926ccea-dfd7-4e08-bd93-7a85bd79797...}	29-06-2023 15:38	Hard Disk Image F...	1,40,05,697...

1 item | 1 item selected | 13.3 GB

Target Machine Virtual Hard disk copy

File Explorer window showing the contents of the 'Cases' folder. The address bar indicates the path: This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases >. The left sidebar shows the navigation pane with 'SDT_x64FREE_EN' selected. The main pane displays a list of files and folders.

Name	Date modified	Type	Size
Analysis	16-07-2023 11:24	File folder	
F	30-06-2023 08:31	File folder	
{0926ccea-dfd7-4e08-bd93-7a85bd79797...}	29-06-2023 15:38	Hard Disk Image F...	1,40,05,697...
2023-06-30T08_30_13_5798095_ConsoleLog	30-06-2023 08:31	Text Document	4 KB
2023-06-30T08_30_13_5798095_CopyLog	30-06-2023 08:31	CSV File	189 KB
2023-06-30T08_30_13_5798095_SkipLog.csv	30-06-2023 08:31	CSV File	9 KB

Paste here the hard disk.



17:42
24-07-2023



- Recycle Bin
- Firefox
- Notepad++
- Event Log Explorer
- Arsenalma... - Shortcut

```
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases
forensics@WIN-BK1Q9542K3L:~$ cd /mnt/c/Cases/
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases$ ls -l
total 15433700
-rwxrwxrwx 1 forensics forensics 3760 Mar 23 22:40 2022-03-23T223835_ConsoleLog.txt
-rwxrwxrwx 1 forensics forensics 195855 Mar 23 22:40 2022-03-23T223835_CopyLog.csv
-rwxrwxrwx 1 forensics forensics 9630 Mar 23 22:40 2022-03-23T223835_SkipLog.csv
drwxrwxrwx 1 forensics forensics 512 Jun 7 17:51 mp3files
drwxrwxrwx 1 forensics forensics 512 Mar 23 22:40
-rwxrwxrwx 1 forensics forensics 7374 May 18 04:37 Notes.docx
-rwxrwxrwx 1 forensics forensics 15803884544 Mar 19 00:13 win10-disk.vhd
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases$ qemu-img convert -O raw win10-disk.vhd win10-disk.raw
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases$
```

qemu-img convert -O raw win10-disk.vhd win10-disk.raw

Using the Following Command converting the disk image.

- Videos
 - Local Disk (C:)
 - CD Drive (D:) VirtualBox Guest Additions
 - Documents (\\.\Device\NFS)
- 10 items 1 item selected



```

forensics@WIN-BK10
forensics@WIN-BK10
total 15433700
-rwxrwxrwx 1 for
-rwxrwxrwx 1 for
drwxrwxrwx 1 for
drwxrwxrwx 1 for
-rwxrwxrwx 1 for
-rwxrwxrwx 1 for
forensics@WIN-BK10
forensics@WIN-BK10

```

File Explorer window titled "Cases" showing the contents of Local Disk (C:) \ Cases. The file "win10-disk.raw" is selected.

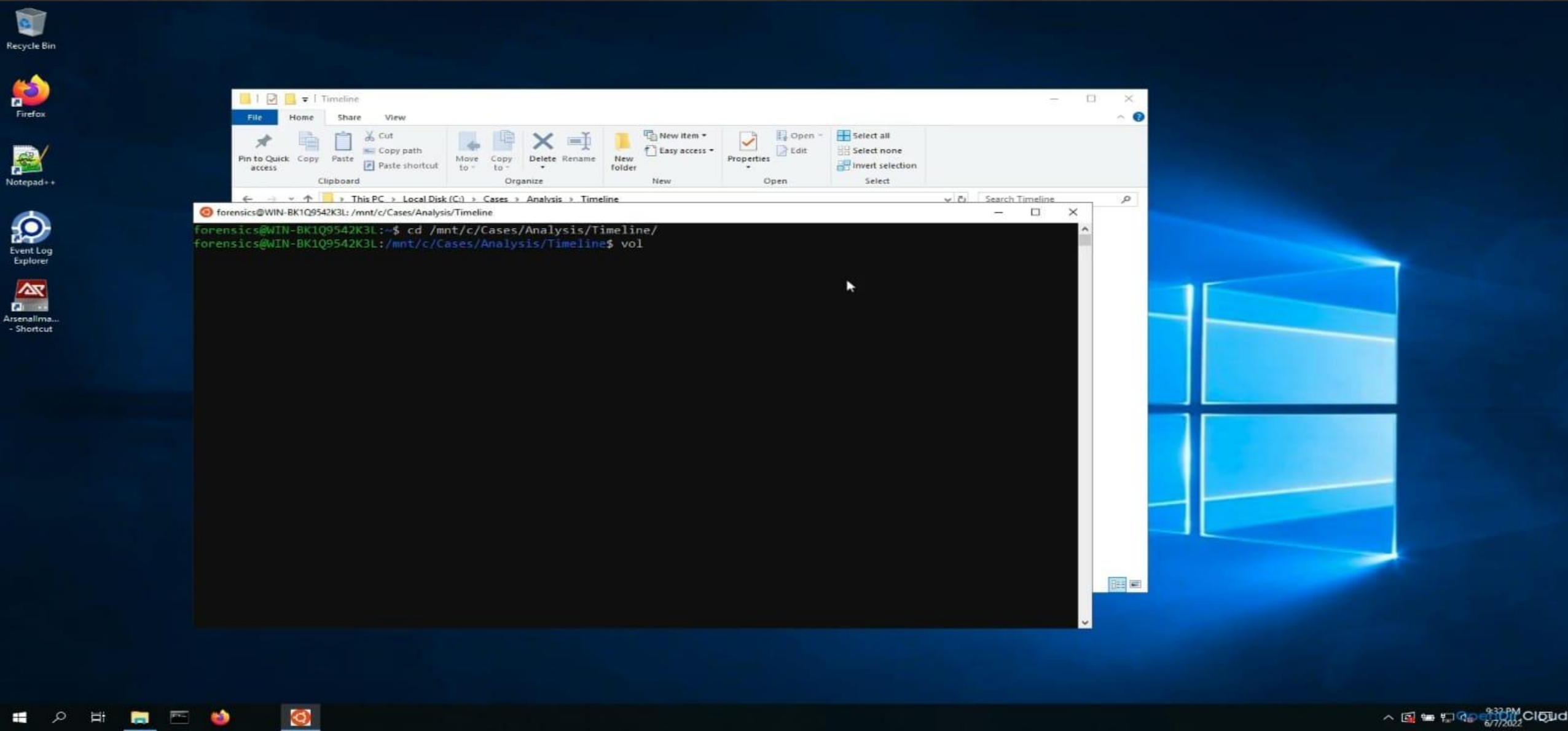
Name	Date modified	Type	Size
Analysis	6/7/2022 5:51 PM	File folder	
E	3/23/2022 10:40 PM	File folder	
2022-03-23T223835_ConsoleLog.txt	3/23/2022 10:40 PM	Text Document	4 KB
2022-03-23T223835_CopyLog.csv	3/23/2022 10:40 PM	CSV File	192 KB
2022-03-23T223835_SkiplLog.csv	3/23/2022 10:40 PM	CSV File	10 KB
Notes.docx	5/18/2022 4:37 AM	Office Open XML ...	8 KB
<input checked="" type="checkbox"/> win10-disk.raw	6/7/2022 9:24 PM	RAW File	41,942,400 ...
win10-disk.vhd	3/19/2022 12:13 AM	Hard Disk Image F...	15,433,481 ...

Disk Image Of the Hard Disk.



Memory timeline creation with Volatility3

Create a folder Timeline . Go to the folder path in ubuntu linux.





Recycle Bin



Firefox



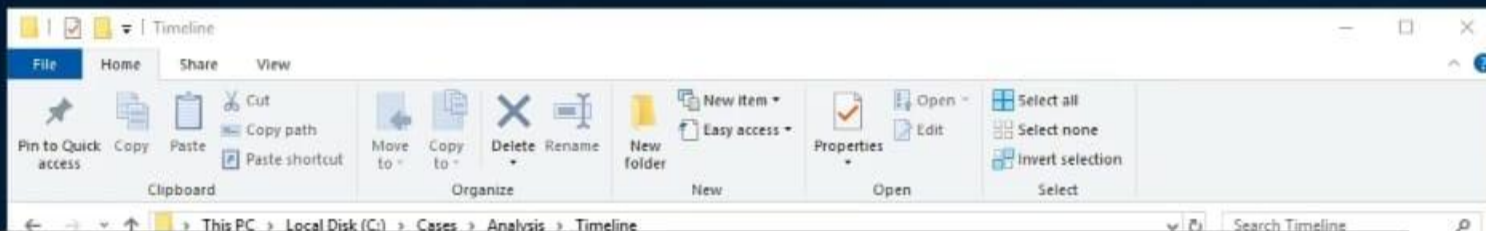
Notepad+



Event Log Explorer



Arsenalima...
- Shortcut



```
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline
forensics@WIN-BK1Q9542K3L:~$ cd /mnt/c/Cases/Analysis/Timeline/
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ vol
vol      volname  volshell
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ vol
vol      volname  volshell
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ vol -h
```

Using vol -h show all plugins in detail.

```
mac.netstat.Netstat      Lists all network connections for all processes.
mac.proc_maps.Maps      Lists process memory ranges that potentially contain injected code.
mac.psaux.PsAux         Recovers program command line arguments.
mac.pslist.PsList       Lists the processes present in a particular mac memory image.
mac.pstree.PsTree       Plugin for listing processes in a tree based on their parent process ID.
mac.socket_filters.Socket_filters
                        Enumerates kernel socket filters.
mac.timers.Timers       Check for malicious kernel timers.
mac.trustedbsd.Trustedbsd
                        Checks for malicious trustedbsd modules
mac.vfsevents.VFSevents
                        Lists processes that are filtering file system events
timeliner.Timeliner    Runs all relevant plugins that provide time related information and orders the results by time.
windows.bigpools.BigPools
                        List big page pools.
windows.callbacks.Callbacks
                        Lists kernel callbacks and notification routines.
windows.cmdline.Cmdline
                        Lists process command line arguments.
windows.crashinfo.Crashinfo
windows.dlllist.Dlllist
                        Lists the loaded modules in a particular windows memory image.
windows.driverirp.DriverIrp
                        List IRPs for drivers in a particular windows memory image.
windows.driverscan.DriverScan
                        Scans for drivers present in a particular windows memory image.
windows.dumpfiles.DumpFiles
                        Dumps cached file contents from Windows memory samples.
windows.envars.Envars
                        Display process environment variables
windows.filescan.FileScan
                        Scans for file objects present in a particular windows memory image.
windows.getservicesids.GetServiceSIDs
                        Lists process token sids.
windows.getsids.GetSIDs
                        Print the SIDs owning each process
windows.handles.Handles
                        Lists process open handles.
windows.info.Info       Show OS & kernel details of the memory sample being analyzed.
windows.malfind.Malfind
                        Lists process memory ranges that potentially contain injected code.
windows.memmap.Memmap
                        Prints the memory map
windows.modscan.ModScan
                        Scans for modules present in a particular windows memory image.
windows.modules.Modules
                        Lists the loaded kernel modules.
windows.mutantscan.MutantScan
```

Show the timeline plugins and gathering the all detail about target memory using timeline plugin.

```
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline
windows.registry.certificates.Certificates
    Lists the certificates in the registry's Certificate Store.
windows.registry.hivelist.HiveList
    Lists the registry hives present in a particular memory image.
windows.registry.hivescan.HiveScan
    Scans for registry hives present in a particular windows memory image.
windows.registry.printkey.PrintKey
    Lists the registry keys under a hive or specific key value.
windows.registry.userassist.UserAssist
    Print userassist registry keys and information.
windows.skeleton_key_check.Skeleton_Key_Check
    Looks for signs of Skeleton Key malware
windows.ssdtd.SSDT
    Lists the system call table.
windows.statistics.Statistics
windows.strings.Strings
    Reads output from the strings command and indicates which process(es) each string belongs to.
windows.svcscan.SvcScan
    Scans for windows services.
windows.symlinkscan.SymlinkScan
    Scans for links present in a particular windows memory image.
windows.vadinfo.VadInfo
    Lists process memory ranges.
windows.vadyarascan.VadYaraScan
    Scans all the Virtual Address Descriptor memory maps using yara.
windows.verinfo.VerInfo
    Lists version information from PE files.
windows.virtmap.VirtMap
    Lists virtual mapped sections.
yarascan.YaraScan
    Scans kernel memory using yara rules (string or file).
```

```
The following plugins could not be loaded (use -vv to see why): volatility3.plugins.windows.cachedump,
volatility3.plugins.windows.hashdump, volatility3.plugins.windows.lsadump
```

```
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline$
```

```
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline$ vol timeliner -h
```

```
Volatility 3 Framework 2.0.1
```

```
usage: volatility timeliner.Timeliner [-h] [--plugins PLUGINS] [--record-config] [--plugin-filter [PLUGIN-FILTER [PLUGIN-FILTER ...]]]
      [--create-bodyfile]
```

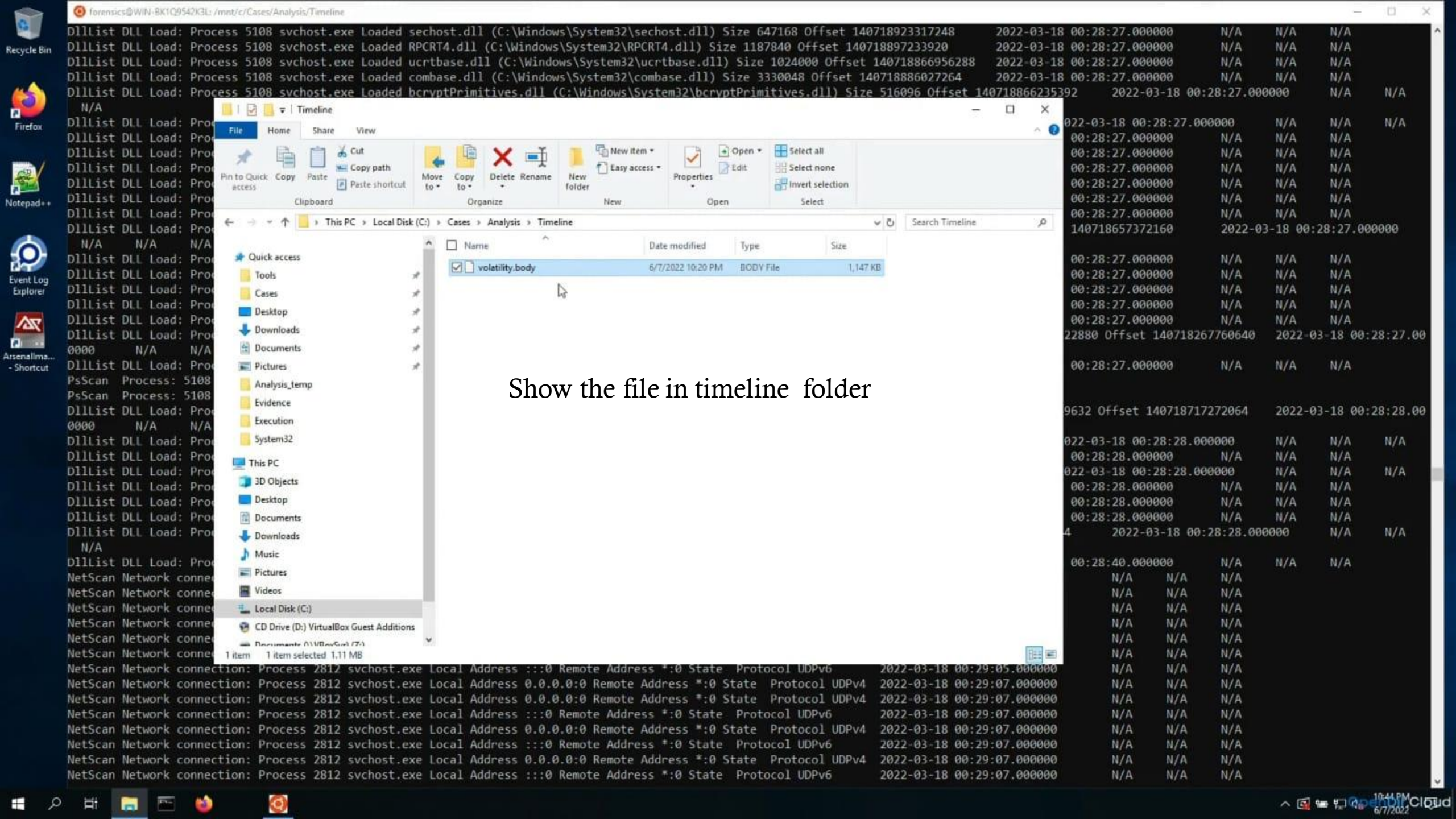
```
optional arguments:
```

```
-h, --help            show this help message and exit
--plugins PLUGINS     Comma separated list of plugins to run
--record-config       Whether to record the state of all the plugins once complete
--plugin-filter [PLUGIN-FILTER [PLUGIN-FILTER ...]]
                    Only run plugins featuring this substring
--create-bodyfile     Whether to create a body file whilst producing results
```

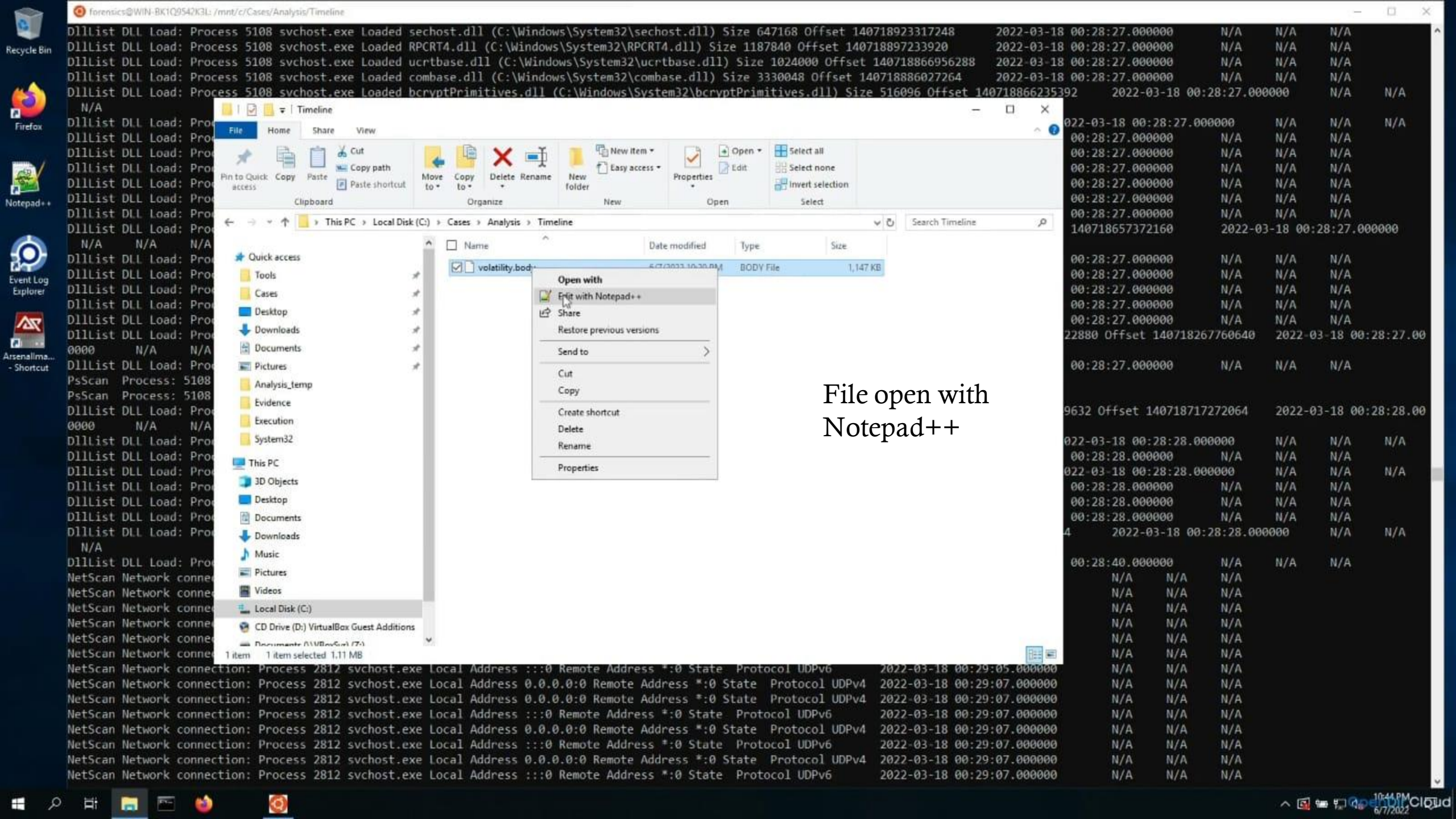
```
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline$ vol -f /mnt/c/Cases/Analysis/Memory/
dlls/                  dlls.txt                win10-memory.raw
```

```
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline$ vol -f /mnt/c/Cases/Analysis/Memory/win10-memory.raw timeliner --create-bodyfile
```

Using this command
and using memory.raw
collect all eventlog and
store the one file.



Show the file in timeline folder



```
Dlllist DLL Load: Process 5108 svchost.exe Loaded sechost.dll (C:\Windows\System32\sechost.dll) Size 647168 Offset 140718923317248 2022-03-18 00:28:27.000000 N/A N/A N/A
Dlllist DLL Load: Process 5108 svchost.exe Loaded RPCRT4.dll (C:\Windows\System32\RPCRT4.dll) Size 1187840 Offset 140718897233920 2022-03-18 00:28:27.000000 N/A N/A N/A
Dlllist DLL Load: Process 5108 svchost.exe Loaded ucrtbase.dll (C:\Windows\System32\ucrtbase.dll) Size 1024000 Offset 140718866956288 2022-03-18 00:28:27.000000 N/A N/A N/A
Dlllist DLL Load: Process 5108 svchost.exe Loaded combase.dll (C:\Windows\System32\combase.dll) Size 3330048 Offset 140718886027264 2022-03-18 00:28:27.000000 N/A N/A N/A
Dlllist DLL Load: Process 5108 svchost.exe Loaded bcryptPrimitives.dll (C:\Windows\System32\bcryptPrimitives.dll) Size 516096 Offset 140718866235392 2022-03-18 00:28:27.000000 N/A N/A
```

Timeline

File Home Share View

Clipboard: Copy, Paste, Copy path, Move to, Copy to, Delete, Rename, New folder, Easy access, Properties, Edit, Select all, Select none, Invert selection

This PC > Local Disk (C:) > Cases > Analysis > Timeline

Name	Date modified	Type	Size
volatility.body	6/7/2022 10:30:34 AM	BODY File	1,147 KB

Open with: Edit with Notepad++, Share, Restore previous versions, Send to, Cut, Copy, Create shortcut, Delete, Rename, Properties

File open with Notepad++

```
NetScan Network connection: Process 2812 svchost.exe Local Address :::0 Remote Address *:0 State Protocol UDPv6 2022-03-18 00:29:05.000000 N/A N/A N/A
NetScan Network connection: Process 2812 svchost.exe Local Address 0.0.0.0:0 Remote Address *:0 State Protocol UDPv4 2022-03-18 00:29:07.000000 N/A N/A N/A
NetScan Network connection: Process 2812 svchost.exe Local Address 0.0.0.0:0 Remote Address *:0 State Protocol UDPv4 2022-03-18 00:29:07.000000 N/A N/A N/A
NetScan Network connection: Process 2812 svchost.exe Local Address :::0 Remote Address *:0 State Protocol UDPv6 2022-03-18 00:29:07.000000 N/A N/A N/A
NetScan Network connection: Process 2812 svchost.exe Local Address 0.0.0.0:0 Remote Address *:0 State Protocol UDPv4 2022-03-18 00:29:07.000000 N/A N/A N/A
NetScan Network connection: Process 2812 svchost.exe Local Address :::0 Remote Address *:0 State Protocol UDPv6 2022-03-18 00:29:07.000000 N/A N/A N/A
NetScan Network connection: Process 2812 svchost.exe Local Address 0.0.0.0:0 Remote Address *:0 State Protocol UDPv4 2022-03-18 00:29:07.000000 N/A N/A N/A
NetScan Network connection: Process 2812 svchost.exe Local Address :::0 Remote Address *:0 State Protocol UDPv6 2022-03-18 00:29:07.000000 N/A N/A N/A
```

```
C:\Cases\Analysis\Timeline\volatility.body - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
NTUSER.DAT.txt SAM.txt SECURITY.txt SOFTWARE.txt SYSTEM.txt UserClass.dat.txt volatility.body.txt
1 |PsList - Process: 4 System (221572833432000) |||1647562205
2 |PsList - Process: 88 Registry (221572834857024) |||1647562199
3 |PsList - Process: 316 smss.exe (221572846485568) |||1647562205
4 |PsList - Process: 408 csrss.exe (221572897677440) |||1647562214
5 |PsList - Process: 484 wininit.exe (221572905160832) |||1647562214
6 |PsList - Process: 492 csrss.exe (221572905239872) |||1647562214
7 |PsList - Process: 544 winlogon.exe (221572905431168) |||1647562214
8 |PsList - Process: 624 services.exe (221572897637696) |||1647562214
9 |PsList - Process: 632 lsass.exe (221572897621120) |||1647562214
10 |PsList - Process: 732 svchost.exe (221572904571648) |||1647562215
11 |PsList - Process: 744 fontdrvhost.ex (221572892942464) |||1647562215
12 |PsList - Process: 752 fontdrvhost.ex (221572892955136) |||1647562215
13 |PsList - Process: 824 svchost.exe (221572905198336) |||1647562215
14 |PsList - Process: 872 svchost.exe (221572905870208) |||1647562215
15 |PsList - Process: 920 svchost.exe (221572906251008) |||1647562215
16 |PsList - Process: 996 dwm.exe (221572912832704) |||1647562215
17 |PsList - Process: 360 svchost.exe (221572913124224) |||1647562216
18 |PsList - Process: 480 svchost.exe (221572913214400) |||1647562216
19 |PsList - Process: 688 svchost.exe (221572913365824) |||1647562216
20 |PsList - Process: 620 svchost.exe (221572913378240) |||1647562216
21 |PsList - Process: 1088 svchost.exe (221572833669312) |||1647562216
22 |PsList - Process: 1124 svchost.exe (221572834099328) |||1647562216
23 |PsList - Process: 1148 svchost.exe (221572834119808) |||1647562216
24 |PsList - Process: 1284 svchost.exe (221572833927296) |||1647562216
25 |PsList - Process: 1296 VBoxService.ex (221572833902720) |||1647562216
26 |PsList - Process: 1316 svchost.exe (221572913996544) |||1647562216
27 |PsList - Process: 1368 svchost.exe (221572914676608) |||1647562216
28 |PsList - Process: 1480 svchost.exe (221572915028736) |||1647562217
29 |PsList - Process: 1500 svchost.exe (221572915286912) |||1647562217
30 |PsList - Process: 1520 svchost.exe (221572915315520) |||1647562217
31 |PsList - Process: 1548 svchost.exe (221572915380992) |||1647562217
32 |PsList - Process: 1620 svchost.exe (221572915549056) |||1647562217
33 |PsList - Process: 1684 MemCompression (221572915695680) |||1647562217
34 |PsList - Process: 1724 svchost.exe (221572915921792) |||1647562217
35 |PsList - Process: 1752 svchost.exe (221572915917568) |||1647562217
36 |PsList - Process: 1852 svchost.exe (221572916216640) |||1647562217
37 |PsList - Process: 1868 svchost.exe (221572915724416) |||1647562217
38 |PsList - Process: 1984 svchost.exe (221572916556672) |||1647562217
39 |PsList - Process: 1144 svchost.exe (221572933685376) |||1647562217
40 |PsList - Process: 1904 svchost.exe (221572933673088) |||1647562217
41 |PsList - Process: 1944 svchost.exe (221572933668992) |||1647562217
42 |PsList - Process: 2120 svchost.exe (221572933656704) |||1647562218
```

Show the All Events.

Creating a Timeline of the disk image with Plaso tools

```
Select forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline

is 2147483648 (2 GiB). If a worker process exceeds this limit it is killed by the main (foreman) process.
--worker_timeout MINUTES, --worker-timeout MINUTES
Number of minutes before a worker process that is not providing status updates is considered inactive. The default timeout is 15.0 minutes. If a worker
process exceeds this timeout it is killed by the main (foreman) process.
--workers WORKERS
Number of worker processes. The default is the number of available system CPUs minus one, for the main (foreman) process.
--sigsegv_handler, --sigsegv-handler
Enables the SIGSEGV handler. WARNING this functionality is experimental and will a deadlock worker process if a real segfault is caught, but not signal
SIGSEGV. This functionality is therefore primarily intended for debugging purposes

profiling arguments:
--profilers PROFILERS_LIST
List of profilers to use by the tool. This is a comma separated list where each entry is the name of a profiler. Use "--profilers list" to list the
available profilers.
--profiling_directory DIRECTORY, --profiling-directory DIRECTORY
Path to the directory that should be used to store the profiling sample files. By default the sample files are stored in the current working directory.
--profiling_sample_rate SAMPLE_RATE, --profiling-sample-rate SAMPLE_RATE
Profiling sample rate (defaults to a sample every 1000 files).

storage arguments:
--storage_file PATH, --storage-file PATH
The path of the storage file. If not specified, one will be made in the form <timestamp>-<source>.plaso
--storage_format FORMAT, --storage-format FORMAT
Format of the storage file, the default is: sqlite. Supported options: sqlite
--task_storage_format FORMAT, --task-storage-format FORMAT
Format for task storage, the default is: sqlite. Supported options: redis, sqlite

Example usage:

Run the tool against a storage media image (full kitchen sink)
log2timeline.py /cases/mycase/storage.plaso imynd.dd

Instead of answering questions, indicate some of the options on the
command line (including data from particular VSS stores).
log2timeline.py --vss_stores 1,2 /cases/plaso_vss.plaso image.E01

And that is how you build a timeline using log2timeline...
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ log2timeline.py --storage-file disk.plaso /mnt/c/Cases/
2022-03-23T223835_ConsoleLog.txt 2022-03-23T223835_SkipLog.csv E/ win10-disk.raw
2022-03-23T223835_CopyLog.csv Analysis/ Notes.docx win10-disk.vhd
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ log2timeline.py --storage-file disk.plaso /mnt/c/Cases/win10-disk.raw
```

Using the disk image
execute this command
and store the output in
one file with name
disk.plaso .



Recycle Bin



Firefox



Notepad++



Event Log Explorer



Arsenalims... - Shortcut

forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline

plaso - log2timeline version 20220428

Source path : /mnt/c/Cases/win10-disk.raw
Source type : storage media image
Processing time : 01:40:20

Tasks:	Queued	Processing	Merging	Abandoned	Total
	0	0	0	0	158051

Identifier	PID	Status	Memory	Sources	Events	File
Main	84	completed	622.5 MiB	158051 (0)	1451337 (0)	
Worker_00	89	idle	415.6 MiB	59935 (0)	763754 (52)	NTFS:\Users\IEUser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\Microsoft
Edge\User\Default\DataStore\Data\nouser1\120712-0049\DBStore\LogFiles\edbtmp.log						
Worker_01	91	idle	479.2 MiB	98115 (0)	687583 (36)	NTFS:\Users\IEUser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\Microsoft
Edge\User\Default\DataStore\Data\nouser1\120712-0049\DBStore\LogFiles\edbres00002.jrs						

Processing completed.

Number of warnings generated while extracting events: 9.

Use pinfo to inspect warnings in more detail.

forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline\$ _

Take a more time for finish the process.

Processing Time
~ 1:40

Activate Windows
Go to Settings to activate Windows.



Recycle Bin



Firefox



Notepad++



Event Log Explorer



Arsenalima... - Shortcut

forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline

plaso - log2timeline version 20220428

Source path : /mnt/c/Cases/win10-disk.raw
Source type : storage media image
Processing time : 01:40:20

Tasks:	Queued	Processing	Merging	Abandoned	Total
	0	0	0	0	158051

Identifier	PID	Status	Memory	Sources	Events	File
Main	84	completed	622.5 MiB	158051 (0)	1451337 (0)	
Worker_00	89	idle	415.6 MiB	59935 (0)	763754 (52)	NTFS:\Users\IEUser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\Microsoft
Worker_01	91	idle	479.2 MiB	98115 (0)	687583 (36)	NTFS:\Users\IEUser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\Microsoft

Processing completed.

Number of warnings generated while extracting events: 9.

Use pininfo to inspect warnings in more detail.

```
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ ls -l
total 684952
-rwxrwxrwx 1 forensics forensics 700153856 Jun  8 02:09 disk.plaso
-rwxrwxrwx 1 forensics forensics      394 Jun  8 02:09 log2timeline-20220608T002923.log.gz
-rwxrwxrwx 1 forensics forensics 1235166 Jun  7 22:46 volatility.body
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ pininfo.py disk.plaso
```

***** Plaso Storage Information *****

Filename : disk.plaso
Format version : 20211121
Serialization format : json

***** Sessions *****

ad8839b4-9583-4854-a69a-248c7b326453 : 2022-06-08T00:29:25.907642+00:00

Show the file in timeline folder and then after open the file and show the all event logs.

Activate Windows
Go to Settings to activate Windows.



Select forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline

```
***** Events generated per parser *****
Parser (plugin) name : Number of events
-----
      amcache : 190
      appcompatcache : 344
      bagmru : 21
      bam : 14
explorer_mountpoints2 : 4
explorer_programscache : 1
      filestat : 632137
      lnk : 453
      mrulist_string : 1
      mrulistex_string : 2
mrulistex_string_and_shell_item : 3
      msie_zone : 36
      networks : 4
olecf_automatic_destinations : 34
      olecf_default : 76
olecf_document_summary : 8
      olecf_summary : 58
      oxml : 14
      pe : 48694
      prefetch : 965
      setupapi : 62
      shell_items : 414
      userassist : 26
      usnjrnl : 237652
windows_boot_execute : 2
      windows_run : 9
      windows_sam_users : 13
      windows_services : 603
      windows_shutdown : 2
      windows_task_cache : 443
      windows_timezone : 1
      windows_typed_urls : 5
      windows_version : 4
      winevtx : 64170
      winlogon : 4
      winreg_default : 464868
      Total : 1451337
-----
```

All event show in this file.

Activate Windows
Go to Settings to activate Windows.

Generating a Super Timeline with plaso tool

```
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline
83 : type: OS, location: /mnt/c/Cases/win10-disk.raw
   : type: RAW
   : type: TSK_PARTITION, location: /p1, part index: 2, start
   : offset: 0x00100000
   : type: NTFS, location:
     \Windows\System32\winevt\Logs\Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx,
     MFT attribute: 2, MFT entry: 81143
78 : type: OS, location: /mnt/c/Cases/win10-disk.raw
   : type: RAW
   : type: TSK_PARTITION, location: /p1, part index: 2, start
   : offset: 0x00100000
   : type: NTFS, location:
     \Windows\System32\winevt\Logs\Microsoft-Windows-WMI-Activity%4Operational.evtx,
     MFT attribute: 2, MFT entry: 82820
76 : type: OS, location: /mnt/c/Cases/win10-disk.raw
   : type: RAW
   : type: TSK_PARTITION, location: /p1, part index: 2, start
   : offset: 0x00100000
   : type: NTFS, location:
     \Windows\System32\winevt\Logs\Microsoft-Windows-PushNotification-Platform%4Operational.evtx,
     MFT attribute: 2, MFT entry: 82965
52 : type: OS, location: /mnt/c/Cases/win10-disk.raw
   : type: RAW
   : type: TSK_PARTITION, location: /p1, part index: 2, start
   : offset: 0x00100000
   : type: NTFS, location:
     \Windows\System32\winevt\Logs\Microsoft-Windows-Bits-Client%4Operational.evtx,
     MFT attribute: 2, MFT entry: 82681
-----
No analysis reports stored.

forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ ls -l
total 684952
-rwxrwxrwx 1 forensics forensics 700153856 Jun  8 02:09 disk.plaso
-rwxrwxrwx 1 forensics forensics      394 Jun  8 02:09 log2timeline-20220608T002923.log.gz
-rwxrwxrwx 1 forensics forensics 1235166 Jun  7 22:46 volatility.body
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ log2timeline.py --parser=mactime --storage-file=disk.plaso volatility.body
```

Merging timelines with mactime parser using this command.

Select forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline

plaso - psort version 20220428

Storage file : disk.plaso

Processing time : 00:06:36

Events:	Filtered	In time slice	Duplicates	MACB grouped	Total
	1318514	0	24	140077	1458958

Identifier	PID	Status	Memory	Events	Tags	Reports
Main	110	completed	315.0 MiB	140444 (0)	0 (0)	0 (0)

Processing completed.

forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline\$

```
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline
plaso - log2timeline version 20220428

Source path      : /mnt/c/Cases/Analysis/Timeline/volatility.body
Source type     : single file
Processing time  : 00:00:02

Identifier      PID      Status      Memory      Sources      Events      File
Main           106     completed  178.0 MiB   1 (0)        7621 (1358) OS:/mnt/c/Cases/Analysis/Timeline/volatility.body

Processing completed.

forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ ls -l
total 688244
-rwxrwxrwx 1 forensics forensics 703524864 Jun  8 02:46 disk.plaso
-rwxrwxrwx 1 forensics forensics    394 Jun  8 02:09 log2timeline-20220608T002923.log.gz
-rwxrwxrwx 1 forensics forensics    177 Jun  8 02:46 log2timeline-20220608T024654.log.gz
-rwxrwxrwx 1 forensics forensics 1235166 Jun  7 22:46 volatility.body
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ psort.py -o l2tcsv -w super-timeline.csv disk.plaso "date > '2022-03-01 00:00:00'"
```

Using this command plaso file convert to csv file. And also create super timeline.

Select forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline

plaso - psort version 20220428

Storage file
Processing time

Events: Filter
131851

Identifier
Main

Processing completed.
forensics@WIN-BK1Q9542

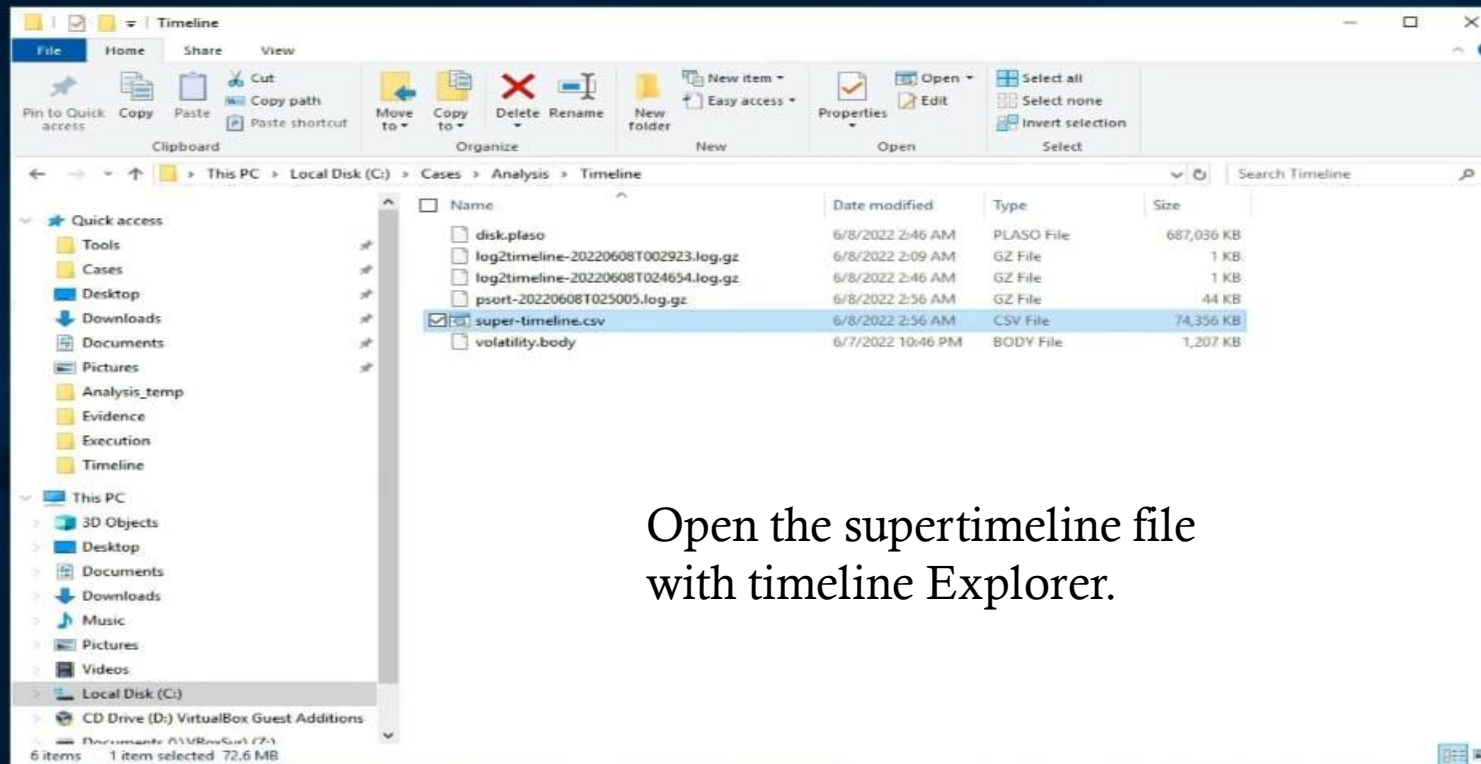
The screenshot shows a Windows File Explorer window titled 'Timeline' with the 'Extract' ribbon tab active. The address bar shows the path: This PC > Local Disk (C:) > Cases > Analysis > Timeline. The main pane displays a list of files with columns for Name, Date modified, Type, and Size. The file 'psort-20220608T025005.log.gz' is selected, highlighted in blue. Other files include 'disk.plaso', 'log2timeline-20220608T002923.log.gz', 'log2timeline-20220608T024654.log.gz', 'super-timeline.csv', and 'volatility.body'. The left sidebar shows the navigation pane with 'Local Disk (C:)' selected.

Name	Date modified	Type	Size
disk.plaso	6/8/2022 2:46 AM	PLASO File	687,036 KB
log2timeline-20220608T002923.log.gz	6/8/2022 2:09 AM	GZ File	1 KB
log2timeline-20220608T024654.log.gz	6/8/2022 2:46 AM	GZ File	1 KB
psort-20220608T025005.log.gz	6/8/2022 2:56 AM	GZ File	44 KB
super-timeline.csv	6/8/2022 2:56 AM	CSV File	74,356 KB
volatility.body	6/7/2022 10:46 PM	BODY File	1,207 KB

Show the two new add file.

Super timeline Analysis

A detailed timeline of everything that occurred on a system, also known as a Super Timeline, can be extremely beneficial in determining what took place in a digital investigation.



Open the supertimeline file with timeline Explorer.

Drag a column header here to group by that column

Enter text to search... Find

Line	Tag	Timestamp	Source Description	Source Name	macb	Inode	Long Description
915	<input type="checkbox"/>	0001-01-01 00:00:00	System - Network Co...	LOG	.a..	46357	SSID: Network Description: Network Connection Type: Wired Default Gateway Mac: 52:54:00:12:35:02 DNS Suffix: <none>
1	<input type="checkbox"/>	2022-03-01 22:10:46	PE Event	PE	...b	126961	PE Type: Dynamic Link Library (DLL)
2	<input type="checkbox"/>	2022-03-01 22:10:47	PE Event	PE	...b	126963	PE Type: Dynamic Link Library (DLL)
3	<input type="checkbox"/>	2022-03-01 22:10:48	PE Event	PE	...b	126965	PE Type: Dynamic Link Library (DLL)
4	<input type="checkbox"/>	2022-03-01 22:10:49	PE Event	PE	...b	126967	PE Type: Dynamic Link Library (DLL)
5	<input type="checkbox"/>	2022-03-01 22:10:49	PE Event	PE	...b	126969	PE Type: Dynamic Link Library (DLL)
6	<input type="checkbox"/>	2022-03-01 22:10:50	PE Event	PE	...b	126971	PE Type: Dynamic Link Library (DLL)
7	<input type="checkbox"/>	2022-03-01 22:10:51	PE Event	PE	...b	126973	PE Type: Dynamic Link Library (DLL)
8	<input type="checkbox"/>	2022-03-01 22:10:52	PE Event	PE	...b	126975	PE Type: Dynamic Link Library (DLL)
9	<input type="checkbox"/>	2022-03-01 22:10:53	PE Event	PE	...b	126977	PE Type: Dynamic Link Library (DLL)
10	<input type="checkbox"/>	2022-03-01 22:11:00	PE Event	PE	...b	126979	PE Type: Dynamic Link Library (DLL)
11	<input type="checkbox"/>	2022-03-01 22:11:13	PE Event	PE	...b	126981	PE Type: Dynamic Link Library (DLL)
12	<input type="checkbox"/>	2022-03-01 22:11:25	PE Event	PE	...b	126983	PE Type: Dynamic Link Library (DLL)
13	<input type="checkbox"/>	2022-03-01 22:11:50	PE Event	PE	...b	126985	PE Type: Dynamic Link Library (DLL)
14	<input type="checkbox"/>	2022-03-01 22:12:13	PE Event	PE	...b	126987	PE Type: Dynamic Link Library (DLL)
15	<input type="checkbox"/>	2022-03-01 22:12:39	PE Event	PE	...b	126989	PE Type: Dynamic Link Library (DLL)
16	<input type="checkbox"/>	2022-03-01 22:12:52	PE Event	PE	...b	126991	PE Type: Dynamic Link Library (DLL)
17	<input type="checkbox"/>	2022-03-01 22:13:07	PE Event	PE	...b	126993	PE Type: Dynamic Link Library (DLL)
18	<input type="checkbox"/>	2022-03-01 22:13:21	PE Event	PE	...b	126995	PE Type: Dynamic Link Library (DLL)
19	<input type="checkbox"/>	2022-03-01 22:13:26	PE Event	PE	...b	126997	PE Type: Dynamic Link Library (DLL)
20	<input type="checkbox"/>	2022-03-01 22:13:30	PE Event	PE	...b	126999	PE Type: Dynamic Link Library (DLL)
21	<input type="checkbox"/>	2022-03-01 22:13:35	PE Event	PE	...b	127001	PE Type: Dynamic Link Library (DLL)
22	<input type="checkbox"/>	2022-03-01 22:13:43	PE Event	PE	...b	127003	PE Type: Dynamic Link Library (DLL)
23	<input type="checkbox"/>	2022-03-01 22:13:47	PE Event	PE	...b	127005	PE Type: Dynamic Link Library (DLL)
24	<input type="checkbox"/>	2022-03-01 22:13:53	PE Event	PE	...b	127007	PE Type: Dynamic Link Library (DLL)
25	<input type="checkbox"/>	2022-03-01 22:13:57	PE Event	PE	...b	127009	PE Type: Dynamic Link Library (DLL)
26	<input type="checkbox"/>	2022-03-01 22:13:59	PE Event	PE	...b	127011	PE Type: Dynamic Link Library (DLL)
27	<input type="checkbox"/>	2022-03-01 22:14:00	PE Event	PE	...b	127013	PE Type: Dynamic Link Library (DLL)
28	<input type="checkbox"/>	2022-03-01 22:14:02	PE Event	PE	...b	127015	PE Type: Dynamic Link Library (DLL)
29	<input type="checkbox"/>	2022-03-01 22:14:05	PE Event	PE	...b	127017	PE Type: Dynamic Link Library (DLL)
30	<input type="checkbox"/>	2022-03-01 22:14:06	PE Event	PE	...b	127019	PE Type: Dynamic Link Library (DLL)
31	<input type="checkbox"/>	2022-03-01 22:14:08	PE Event	PE	...b	127021	PE Type: Dynamic Link Library (DLL)
32	<input type="checkbox"/>	2022-03-01 22:14:10	PE Event	PE	...b	127023	PE Type: Dynamic Link Library (DLL)
33	<input type="checkbox"/>	2022-03-01 22:14:11	PE Event	PE	...b	127025	PE Type: Dynamic Link Library (DLL)
34	<input type="checkbox"/>	2022-03-01 22:14:12	PE Event	PE	...b	127027	PE Type: Dynamic Link Library (DLL)
35	<input type="checkbox"/>	2022-03-01 22:14:13	PE Event	PE	...b	127029	PE Type: Dynamic Link Library (DLL)

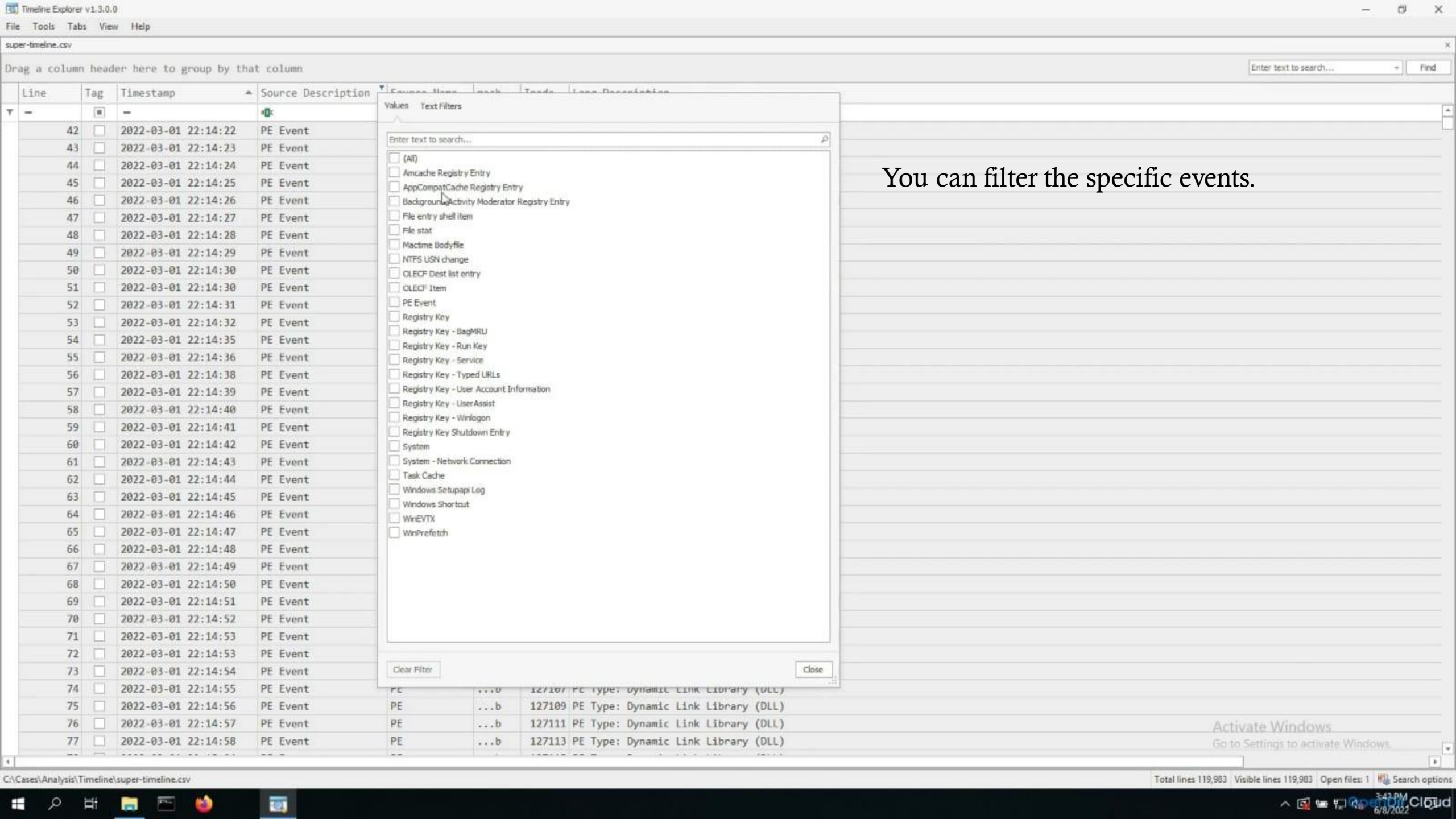
Show All events.

Activate Windows
Go to Settings to activate Windows.

Drag a column header here to group by that column

Enter text to search... Find

Line	Tag	Timestamp	Source Description	Source Name	macb	Inode	Long Description
66	<input type="checkbox"/>	2022-03-01 22:14:48	PE Event	PE	...b	127091	PE Type: Dynamic Link Library (DLL)
67	<input type="checkbox"/>	2022-03-01 22:14:49	PE Event	PE	...b	127093	PE Type: Dynamic Link Library (DLL)
68	<input type="checkbox"/>	2022-03-01 22:14:50	PE Event	PE	...b	127095	PE Type: Dynamic Link Library (DLL)
69	<input type="checkbox"/>	2022-03-01 22:14:51	PE Event	PE	...b	127097	PE Type: Dynamic Link Library (DLL)
70	<input type="checkbox"/>	2022-03-01 22:14:52	PE Event	PE	...b	127099	PE Type: Dynamic Link Library (DLL)
71	<input type="checkbox"/>	2022-03-01 22:14:53	PE Event	PE	...b	127101	PE Type: Dynamic Link Library (DLL)
72	<input type="checkbox"/>	2022-03-01 22:14:53	PE Event	PE	...b	127103	PE Type: Dynamic Link Library (DLL)
73	<input type="checkbox"/>	2022-03-01 22:14:54	PE Event	PE	...b	127105	PE Type: Dynamic Link Library (DLL)
74	<input type="checkbox"/>	2022-03-01 22:14:55	PE Event	PE	...b	127107	PE Type: Dynamic Link Library (DLL)
75	<input type="checkbox"/>	2022-03-01 22:14:56	PE Event	PE	...b	127109	PE Type: Dynamic Link Library (DLL)
76	<input type="checkbox"/>	2022-03-01 22:14:57	PE Event	PE	...b	127111	PE Type: Dynamic Link Library (DLL)
77	<input type="checkbox"/>	2022-03-01 22:14:58	PE Event	PE	...b	127113	PE Type: Dynamic Link Library (DLL)
78	<input type="checkbox"/>	2022-03-01 22:15:04	PE Event	PE	...b	127115	PE Type: Dynamic Link Library (DLL)
79	<input type="checkbox"/>	2022-03-01 22:15:18	PE Event	PE	...b	127117	PE Type: Dynamic Link Library (DLL)
80	<input type="checkbox"/>	2022-03-01 22:15:29	PE Event	PE	...b	127119	PE Type: Dynamic Link Library (DLL)
81	<input type="checkbox"/>	2022-03-01 22:15:37	PE Event	PE	...b	127121	PE Type: Dynamic Link Library (DLL)
82	<input type="checkbox"/>	2022-03-01 22:15:46	PE Event	PE	...b	127123	PE Type: Dynamic Link Library (DLL)
83	<input type="checkbox"/>	2022-03-01 22:15:57	PE Event	PE	...b	127125	PE Type: Dynamic Link Library (DLL)
84	<input type="checkbox"/>	2022-03-01 22:16:10	PE Event	PE	...b	127127	PE Type: Dynamic Link Library (DLL)
85	<input type="checkbox"/>	2022-03-01 22:30:02	PE Event	PE	...b	82809	PE Type: Executable (EXE) Import hash: c757b6532bf3304f2e1da07efe23042e
86	<input type="checkbox"/>	2022-03-01 22:30:02	PE Event	PE	...b	89341	PE Type: Executable (EXE) Import hash: c757b6532bf3304f2e1da07efe23042e
87	<input type="checkbox"/>	2022-03-05 03:19:27	PE Event	PE	...b	32865	PE Type: Executable (EXE) Import hash: 73effd46557538d5fa5561eee3ffc59c
88	<input type="checkbox"/>	2022-03-09 16:48:30	PE Event	PE	m...	54463	PE Type: Dynamic Link Library (DLL) [DIRECTORY_ENTRY_EXPORT] DLL name: USERMGRCLI.dll Import hash: fd490a0262febd37990bdb445c01509
89	<input type="checkbox"/>	2022-03-09 16:48:30	PE Event	PE	m...	54463	PE Type: Dynamic Link Library (DLL) [DIRECTORY_ENTRY_EXPORT] DLL name: USERMGRCLI.dll Import hash: fd490a0262febd37990bdb445c01509
90	<input type="checkbox"/>	2022-03-09 16:48:30	PE Event	PE	...b	54463	PE Type: Dynamic Link Library (DLL) Import hash: fd490a0262febd37990bdb445c01509
91	<input type="checkbox"/>	2022-03-09 16:48:30	PE Event	PE	...b	54463	PE Type: Dynamic Link Library (DLL) Import hash: fd490a0262febd37990bdb445c01509
92	<input type="checkbox"/>	2022-03-11 19:30:07	File stat	FILE	m..b	0	NTFS:\Users\IEUser\AppData\Local\Temp\wctFD02.tmp Type: file
93	<input type="checkbox"/>	2022-03-11 19:33:44	File stat	FILE	m..b	0	NTFS:\Users\IEUser\AppData\Local\Temp\wctF1F5.tmp Type: file
94	<input type="checkbox"/>	2022-03-14 18:18:04	PE Event	PE	...b	82876	PE Type: Dynamic Link Library (DLL)
95	<input type="checkbox"/>	2022-03-14 18:18:04	PE Event	PE	...b	82878	PE Type: Dynamic Link Library (DLL)
96	<input type="checkbox"/>	2022-03-14 18:53:38	File stat	FILE	ma..b	0	NTFS:\Users\IEUser\AppData\Local\Microsoft\Windows\Notifications\wpn1dm\1c7f31e8.png Type: file
97	<input type="checkbox"/>	2022-03-14 19:14:17	PE Event	PE	...b	32881	PE Type: Executable (EXE) Import hash: 73effd46557538d5fa5561eee3ffc59c
98	<input type="checkbox"/>	2022-03-14 19:14:17	PE Event	PE	...b	32874	PE Type: Executable (EXE) Import hash: 73effd46557538d5fa5561eee3ffc59c
99	<input type="checkbox"/>	2022-03-15 16:56:35	PE Event	PE	m...	40112	PE Type: Dynamic Link Library (DLL) [DIRECTORY_ENTRY_EXPORT] DLL name: Qdvd.dll Import hash: 4a828507e62d541bc643dd70e74340c8
100	<input type="checkbox"/>	2022-03-15 16:56:35	PE Event	PE	m...	40112	PE Type: Dynamic Link Library (DLL) [DIRECTORY_ENTRY_EXPORT] DLL name: Qdvd.dll Import hash: 4a828507e62d541bc643dd70e74340c8
101	<input type="checkbox"/>	2022-03-15 16:56:35	PE Event	PE	...b	40112	PE Type: Dynamic Link Library (DLL) Import hash: 4a828507e62d541bc643dd70e74340c8



You can filter the specific events.

Super timeline Analysis Malicious Events

You can show all events

Timeline Explorer v1.3.0.0
 File Tools Tabs View Help
 super-timeline.csv

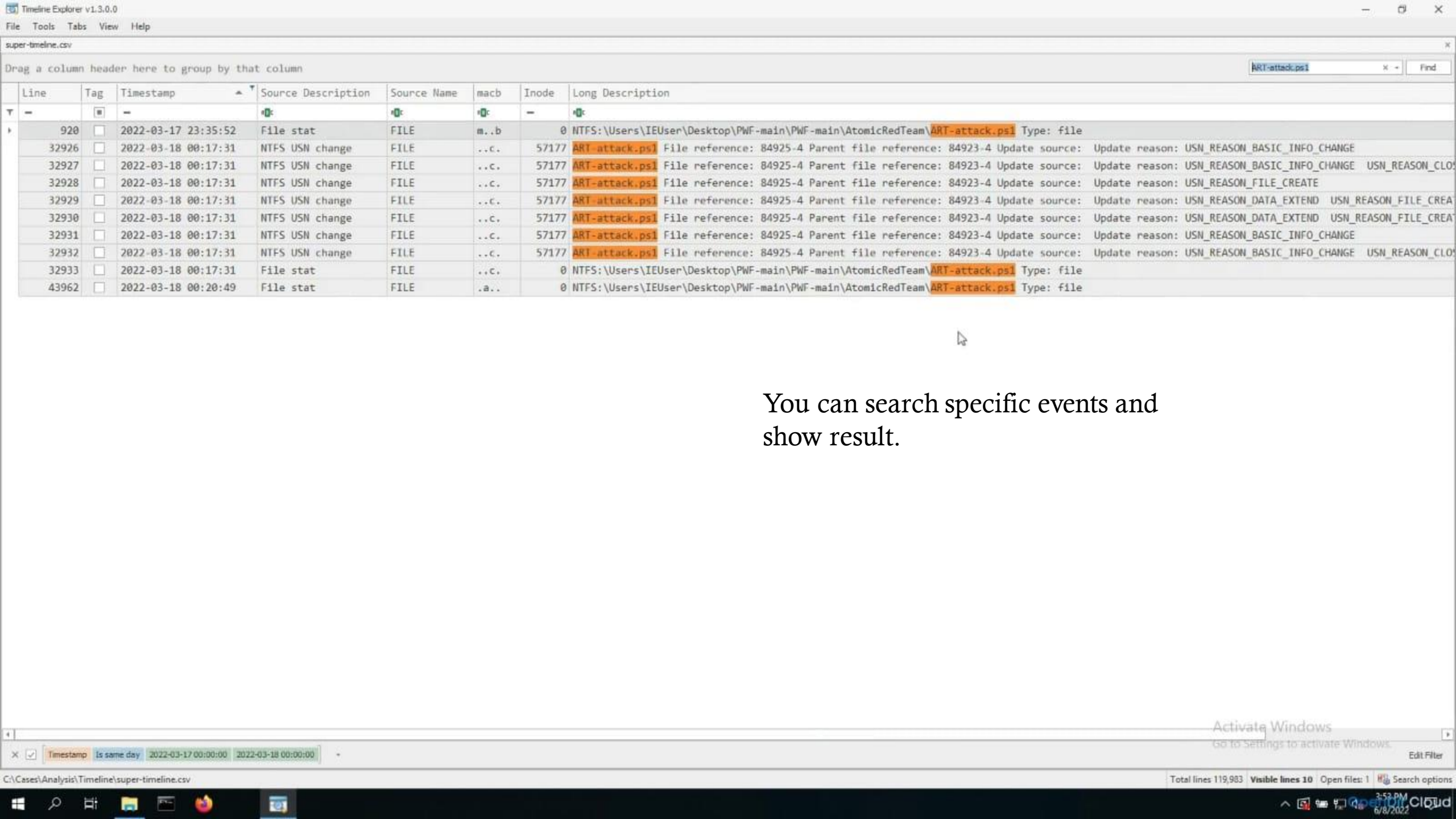
Drag a column header here to group by that column

Line	Tag	Timestamp	Source Description	Source Name	macb	Inode	Long Description
128	<input type="checkbox"/>	2022-03-17 01:04:57	NTFS USN change	FILE	..c.	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
129	<input type="checkbox"/>	2022-03-17 01:04:57	NTFS USN change	FILE	..c.	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
130	<input type="checkbox"/>	2022-03-17 01:04:58	NTFS USN change	FILE	..c.	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
131	<input type="checkbox"/>	2022-03-17 01:04:58	NTFS USN change	FILE	..c.	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
132	<input type="checkbox"/>	2022-03-17 01:04:58	NTFS USN change	FILE	..c.	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
133	<input type="checkbox"/>	2022-03-17 01:04:58	NTFS USN change	FILE	..c.	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
134	<input type="checkbox"/>	2022-03-17 01:05:03	NTFS USN change	FILE	..c.	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
135	<input type="checkbox"/>	2022-03-17 01:05:03	NTFS USN change	FILE	..c.	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
136	<input type="checkbox"/>	2022-03-17 01:05:03	NTFS USN change	FILE	..c.	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
137	<input type="checkbox"/>	2022-03-17 01:05:03	NTFS USN change	FILE	..c.	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
138	<input type="checkbox"/>	2022-03-17 01:05:03	NTFS USN change	FILE	..c.	57177	EtwRTUBPM.etl File reference: 3495-4 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_FILE_CREATE
139	<input type="checkbox"/>	2022-03-17 01:05:03	NTFS USN change	FILE	..c.	57177	EtwRTUBPM.etl File reference: 3495-4 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_FILE_CREAT
140	<input type="checkbox"/>	2022-03-17 01:05:03	NTFS USN change	FILE	..c.	57177	EtwRTDiagLog.etl File reference: 80516-3 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
141	<input type="checkbox"/>	2022-03-17 01:05:03	NTFS USN change	FILE	..c.	57177	EtwRTDiagLog.etl File reference: 80516-3 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_DAT
142	<input type="checkbox"/>	2022-03-17 01:05:03	NTFS USN change	FILE	..c.	57177	EtwRTEventLog-System.etl File reference: 80517-3 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
143	<input type="checkbox"/>	2022-03-17 01:05:03	NTFS USN change	FILE	..c.	57177	EtwRTEventLog-System.etl File reference: 80517-3 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_RE
144	<input type="checkbox"/>	2022-03-17 01:05:03	NTFS USN change	FILE	..c.	57177	BCD.LOG File reference: 80504-3 Parent file reference: 80374-3 Update source: Update reason: USN_REASON_DATA_OVERWRITE
145	<input type="checkbox"/>	2022-03-17 01:05:04	NTFS USN change	FILE	..c.	57177	BCD File reference: 80503-3 Parent file reference: 80374-3 Update source: Update reason: USN_REASON_DATA_OVERWRITE
146	<input type="checkbox"/>	2022-03-17 01:05:04	NTFS USN change	FILE	..c.	57177	EtwRTUBPM.etl File reference: 3495-4 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_FILE_CREAT
147	<input type="checkbox"/>	2022-03-17 01:05:04	NTFS USN change	FILE	..c.	57177	EtwRTDiagLog.etl File reference: 80516-3 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_DAT
148	<input type="checkbox"/>	2022-03-17 01:05:04	NTFS USN change	FILE	..c.	57177	EtwRTEventLog-System.etl File reference: 80517-3 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_RE
149	<input type="checkbox"/>	2022-03-17 01:05:04	NTFS USN change	FILE	..c.	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
150	<input type="checkbox"/>	2022-03-17 01:05:04	NTFS USN change	FILE	..c.	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
151	<input type="checkbox"/>	2022-03-17 01:05:04	NTFS USN change	FILE	..c.	57177	BCD File reference: 80503-3 Parent file reference: 80374-3 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
152	<input type="checkbox"/>	2022-03-17 01:05:04	NTFS USN change	FILE	..c.	57177	BCD.LOG File reference: 80504-3 Parent file reference: 80374-3 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
153	<input type="checkbox"/>	2022-03-17 15:26:04	PE Event	PE	m...	41640	PE Type: Dynamic Link Library (DLL) [DIRECTORY_ENTRY_EXPORT] DLL name: XboxGipRadioManager.dll Import hash: 5d628e9abd82a65cfa9cdf396f6eb2aa
154	<input type="checkbox"/>	2022-03-17 15:26:04	PE Event	PE	m...	41640	PE Type: Dynamic Link Library (DLL) [DIRECTORY_ENTRY_EXPORT] DLL name: XboxGipRadioManager.dll Import hash: 5d628e9abd82a65cfa9cdf396f6eb2aa
155	<input type="checkbox"/>	2022-03-17 15:26:04	PE Event	PE	...b	41640	PE Type: Dynamic Link Library (DLL) Import hash: 5d628e9abd82a65cfa9cdf396f6eb2aa
156	<input type="checkbox"/>	2022-03-17 15:26:04	PE Event	PE	...b	41640	PE Type: Dynamic Link Library (DLL) Import hash: 5d628e9abd82a65cfa9cdf396f6eb2aa
157	<input type="checkbox"/>	2022-03-17 16:10:41	PE Event	PE	...b	82877	PE Type: Dynamic Link Library (DLL)
158	<input type="checkbox"/>	2022-03-17 16:10:41	PE Event	PE	...b	82879	PE Type: Dynamic Link Library (DLL)
159	<input type="checkbox"/>	2022-03-17 16:17:09	PE Event	PE	...b	127811	PE Type: Dynamic Link Library (DLL)
160	<input type="checkbox"/>	2022-03-17 16:17:40	PE Event	PE	...b	127822	PE Type: Dynamic Link Library (DLL)
161	<input type="checkbox"/>	2022-03-17 16:27:16	AppCompatCache Regi...	REG	...	42071	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] Cached entry: 7 Path: C:\AtomicRedTeam\atomics\T1543.003\bin\A
162	<input type="checkbox"/>	2022-03-17 16:27:16	File stat	FILE	m...	0	NTFS:\AtomicRedTeam\atomics\Indexes\Attack-Navigator-Layers\art-navigator-layer-azure-ad.json Type: file

Timestamp: Is same day 2022-03-17 00:00:00 2022-03-18 00:00:00

C:\Cases\Analysis\Timeline\super-timeline.csv Total lines 119,903 Visible lines 98,243 Open file: 1 Search options

3:53 PM 6/8/2022



Timeline Explorer v1.3.0.0

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

atomicservice.exe x Find

Line	Tag	Timestamp	Source Description	Source Name	macb	Inode	Long Description
161		2022-03-17 16:27:16	AppCompatCache Regi...	REG	...	42071	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] Cached entry: 7 Path: C:\AtomicRedTeam\atomic\T1543.003\bin\Atom...
679		2022-03-17 16:27:16	File stat	FILE	m...	0	NTFS:\AtomicRedTeam\atomic\T1543.003\bin\AtomicService.exe Type: file
64767		2022-03-18 00:23:59	NTFS USN change	FILE	..c.	57177	AtomicService.exe File reference: 126258-2 Parent file reference: 126257-2 Update source: Update reason: USN_REASON_FILE_CREATE
64768		2022-03-18 00:23:59	NTFS USN change	FILE	..c.	57177	AtomicService.exe File reference: 126258-2 Parent file reference: 126257-2 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_FILE
64769		2022-03-18 00:23:59	NTFS USN change	FILE	..c.	57177	AtomicService.exe File reference: 126258-2 Parent file reference: 126257-2 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_FILE
64770		2022-03-18 00:23:59	NTFS USN change	FILE	..c.	57177	AtomicService.exe File reference: 126258-2 Parent file reference: 126257-2 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE
64771		2022-03-18 00:23:59	NTFS USN change	FILE	..c.	57177	AtomicService.exe File reference: 126258-2 Parent file reference: 126257-2 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE USN_REASON
64774		2022-03-18 00:23:59	File stat	FILE	..cb	0	NTFS:\AtomicRedTeam\atomic\T1543.003\bin\AtomicService.exe Type: file
64786		2022-03-18 00:23:59	WinEVTX	EVT	m..b	89021	[11 / 0x000b] Source Name: Microsoft-Windows-Sysmon Strings: ['EXE' '2022-03-18 00:23:59.239' '{747F3D96-D020-6233-6B01-000000001200}' '6988'
76958		2022-03-18 00:25:36	Mactime Bodyfile	FILE	..b	0	DllList - DLL Load: Process 6572 AtomicService. Loaded AtomicService.exe (C:\AtomicRedTeam\atomic\T1543.003\bin\AtomicService.exe) Size 32768 Of
76996		2022-03-18 00:25:36	WinE	EVT	m..b	89021	[1 / 0x0001] Source Name: Microsoft-Windows-Sysmon Strings: ['- '2022-03-18 00:25:36.418' '{747F3D96-D180-6233-FE01-000000001200}' '3760' 'C
77000		2022-03-18 00:25:36	WinE	EVT	m..b	89021	[1 / 0x0001] Source Name: Microsoft-Windows-Sysmon Strings: ['- '2022-03-18 00:25:36.619' '{747F3D96-D180-6233-0002-000000001200}' '5176' 'C
77001		2022-03-18 00:25:36	WinE	EVT	m..b	7799	[7045 / 0x1b85] Source Name: Service Control Manager Strings: ['AtomicTestService_CMD' 'C:\AtomicRedTeam\atomic\T1543.003\bin\AtomicServic
77002		2022-03-18 00:25:36	Regi	REG	...	0071	[HKEY_LOCAL_MACHINE\System\ControlSet001\Services\AtomicTestService_CMD] Type: Service - Own Process (0x10) Start: Manual (3) Image path: C:\Atom
77004		2022-03-18 00:25:36	WinE	EVT	m..b	0021	[13 / 0x000d] Source Name: Microsoft-Windows-Sysmon Strings: ['T1031 T1050' 'SetValue' '2022-03-18 00:25:36.676' '{747F3D96-CDE6-6233-0B00-000
77006		2022-03-18 00:25:36	WinE	EVT	m..b	0021	[1 / 0x0001] Source Name: Microsoft-Windows-Sysmon Strings: ['- '2022-03-18 00:25:36.704' '{747F3D96-D180-6233-0102-000000001200}' '2168' 'C
77007		2022-03-18 00:25:36	WinP	EVT	m..b	1874	Prefetch [ATOMICSERVICE.EXE] was executed - run count 1 path hints: \ATOMICREDTEAM\TMP\ATOMIC RED TEAM MASTER\ATOMICS\T1543.003\BIN\ATOMICSERVICE
77008		2022-03-18 00:25:36	WinE	EVT	m..b	0021	[1 / 0x0001] Source Name: Microsoft-Windows-Sysmon Strings: ['- '2022-03-18 00:25:36.805' '{747F3D96-D180-6233-0202-000000001200}' '6572' 'C
77383		2022-03-18 00:25:47	NTFS	FILE	..c.	7177	ATOMICSERVICE.EXE-CFFBD82A.pf File reference: 82874-5 Parent file reference: 80798-1 Update source: Update reason: USN_REASON_FILE_CREATE
77384		2022-03-18 00:25:47	NTFS	FILE	..c.	7177	ATOMICSERVICE.EXE-CFFBD82A.pf File reference: 82874-5 Parent file reference: 80798-1 Update source: Update reason: USN_REASON_DATA_EXTEND USN_R
77385		2022-03-18 00:25:47	NTFS	FILE	..c.	7177	ATOMICSERVICE.EXE-CFFBD82A.pf File reference: 82874-5 Parent file reference: 80798-1 Update source: Update reason: USN_REASON_DATA_EXTEND USN_R
77386		2022-03-18 00:25:47	File stat	FILE	macb	0	NTFS:\Windows\Prefetch\ATOMICSERVICE.EXE-CFFBD82A.pf Type: file
78073		2022-03-18 00:26:00	File stat	FILE	.a..	0	NTFS:\AtomicRedTeam\atomic\T1543.003\bin\AtomicService.exe Type: file
97024		2022-03-18 22:18:56	Registry Key	REG	m..	46357	[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\CIT\Module\Microsoft.NET\Framework64\v4.0.30319\clr.dll] \DeviceV
97514		2022-03-18 22:18:58	NTFS USN change	FILE	..c.	57177	AtomicService.exe.log File reference: 32823-6 Parent file reference: 115206-3 Update source: Update reason: USN_REASON_FILE_CREATE
97515		2022-03-18 22:18:58	NTFS USN change	FILE	..c.	57177	AtomicService.exe.log File reference: 32823-6 Parent file reference: 115206-3 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_F
97516		2022-03-18 22:18:58	NTFS USN change	FILE	..c.	57177	AtomicService.exe.log File reference: 32823-6 Parent file reference: 115206-3 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_F
97518		2022-03-18 22:18:58	File stat	FILE	macb	0	NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\AtomicService.exe.log Type: file
97522		2022-03-18 22:18:58	WinEVTX	EVT	m..b	89021	[11 / 0x000b] Source Name: Microsoft-Windows-Sysmon Strings: ['ProcessHostingdotNETCode' '2022-03-18 22:18:58.353' '{747F3D96-D180-6233-0202-000

Legend (for supported timeline formats)

- FILE OPENING
- WEB HISTORY
- DELETED DATA
- EXECUTION
- LOG FILE

Using colorcode you know about execution on events.

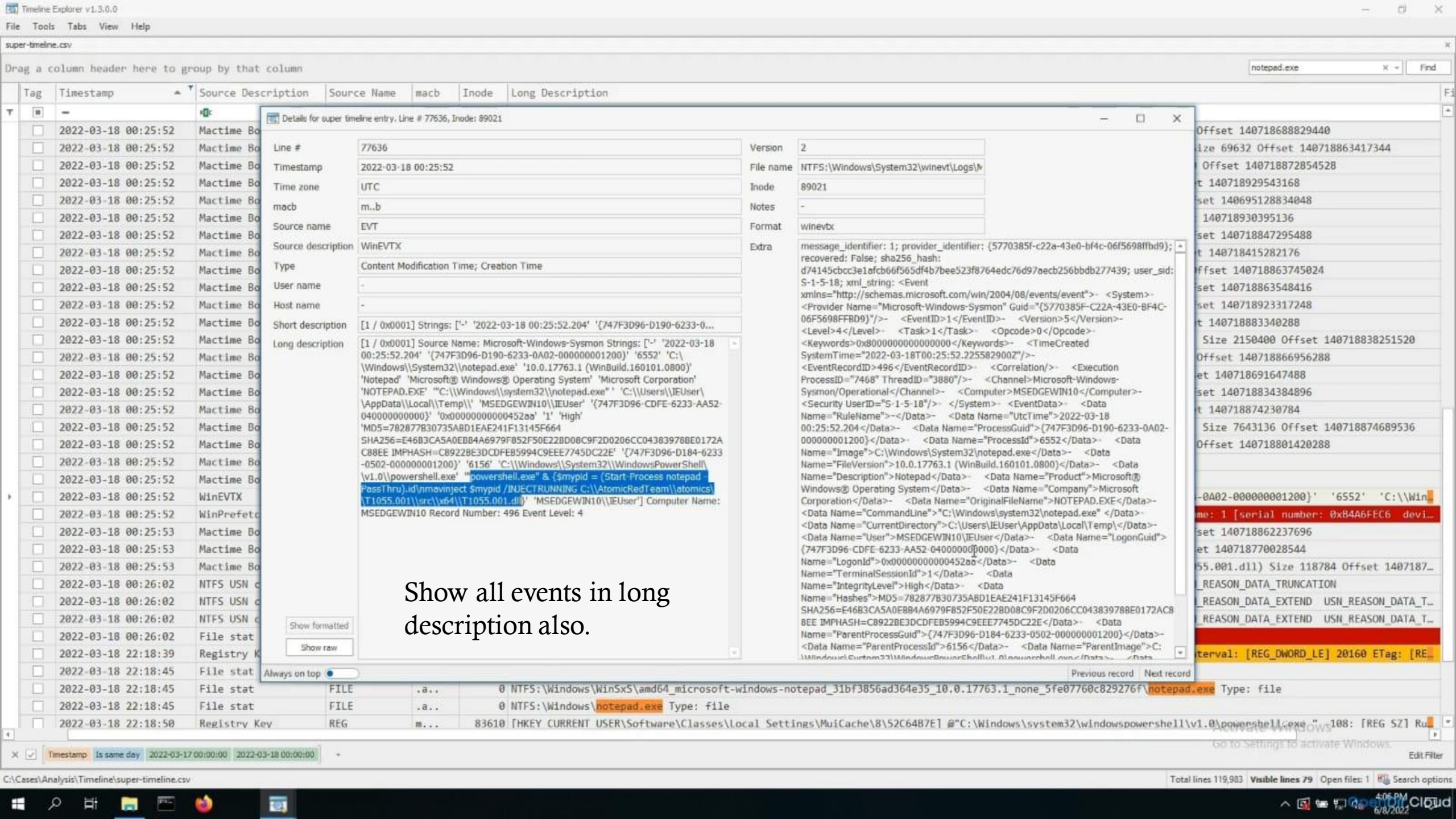
Activate Windows
Go to Settings to activate Windows.

Timestamp Is same day 2022-03-17 00:00:00 2022-03-18 00:00:00

C:\Cases\Analysis\Timeline\super-timeline.csv

Total lines 119,983 Visible lines 29 Open files: 1 Search options

6:01 PM 6/8/2022



Show all events in long description also.

Reporting types and consideration

Reporting Considerations

1. Establish expectations in the beginning!
2. Consider the audience that you are targeting.
3. Alternative Explanations.
4. Actionable Information.

Types of Reporting

Forensic Report - Legal Cases

High-level presentation – Executive debriefs , Q &A documents

System Timeline – Events listed in temporal order

Etc. – Resolving Tickets like some proof screen shorts

Thanks for *Attending* This Session