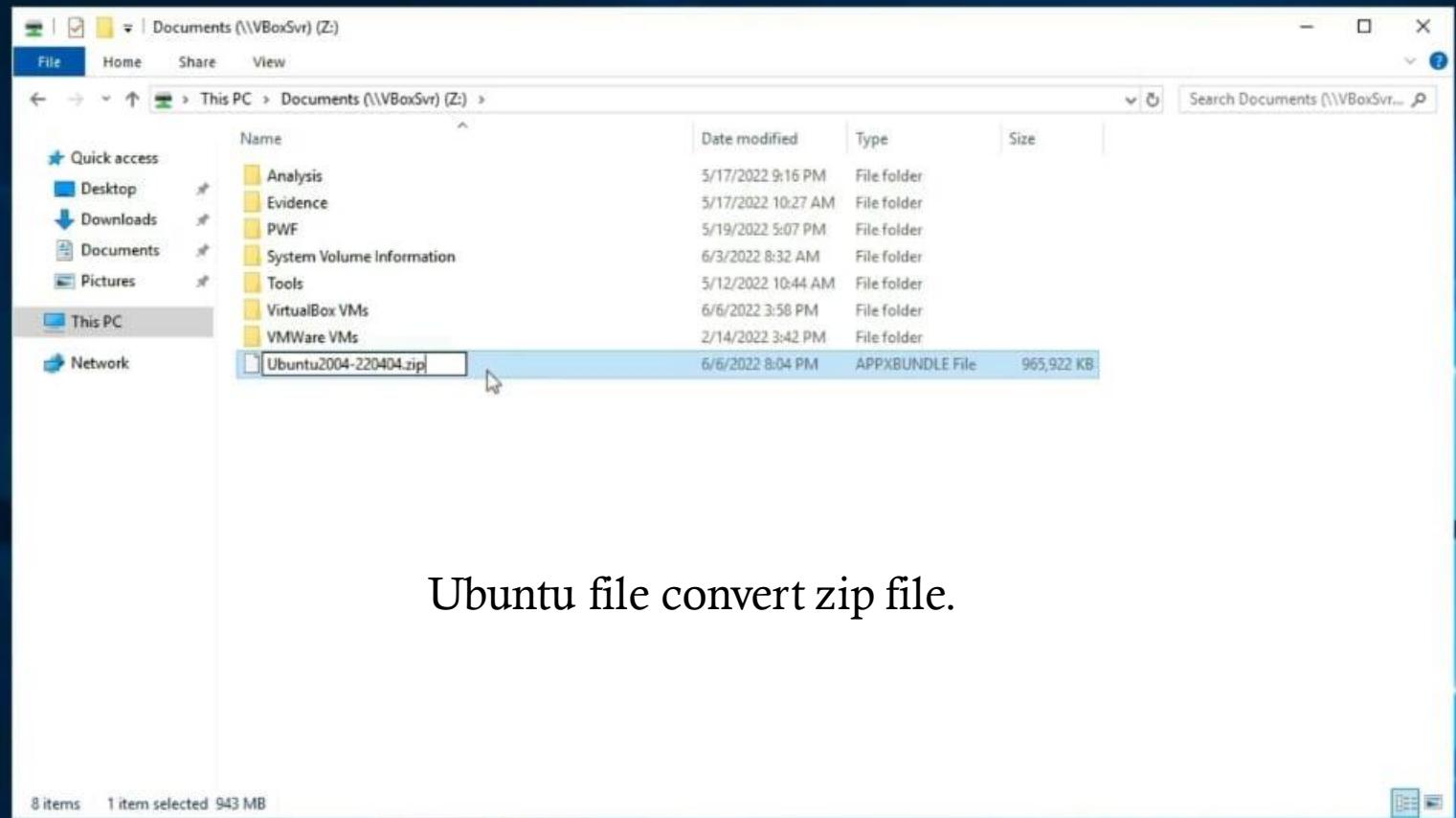


# Windows Forensic

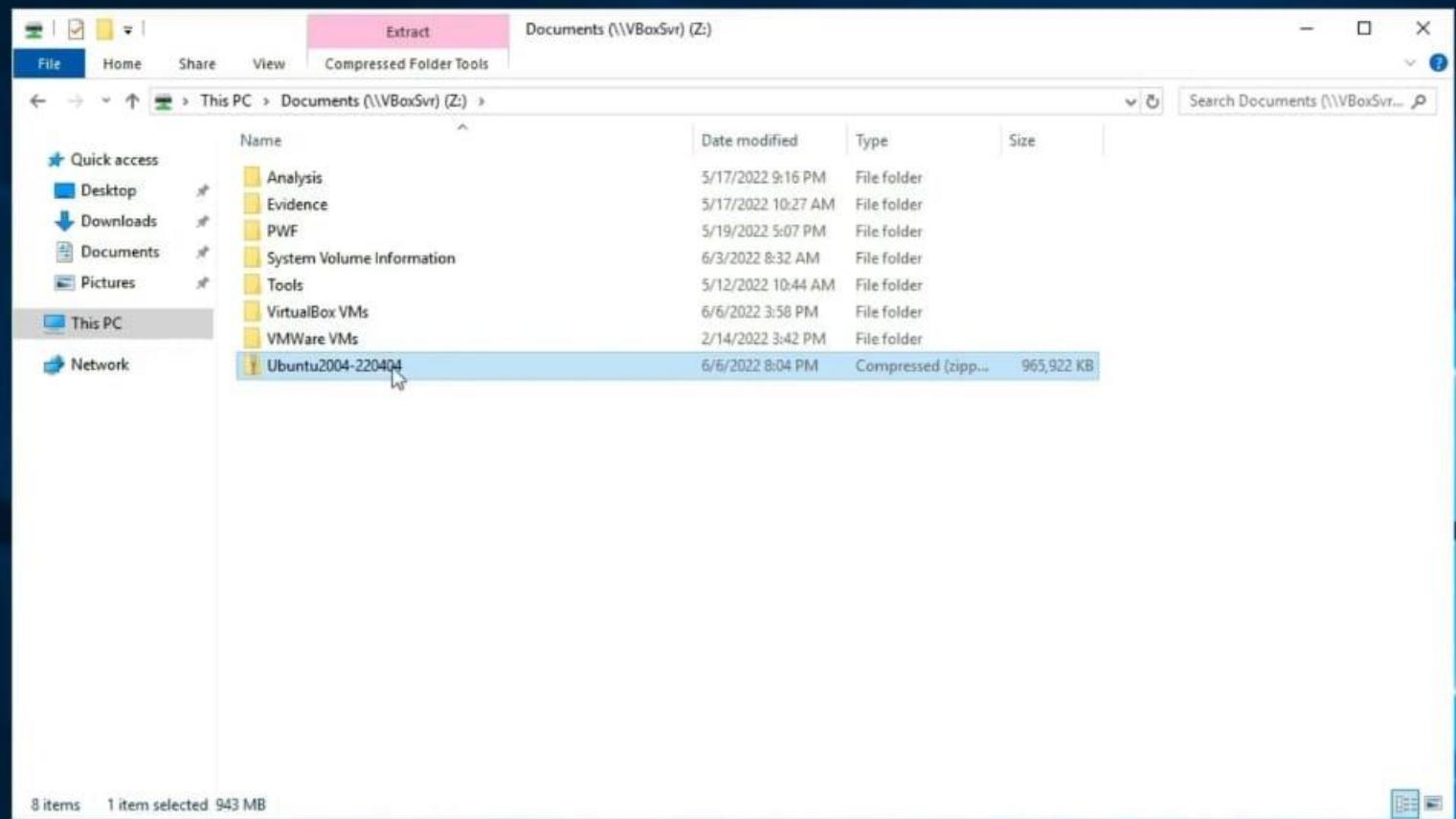


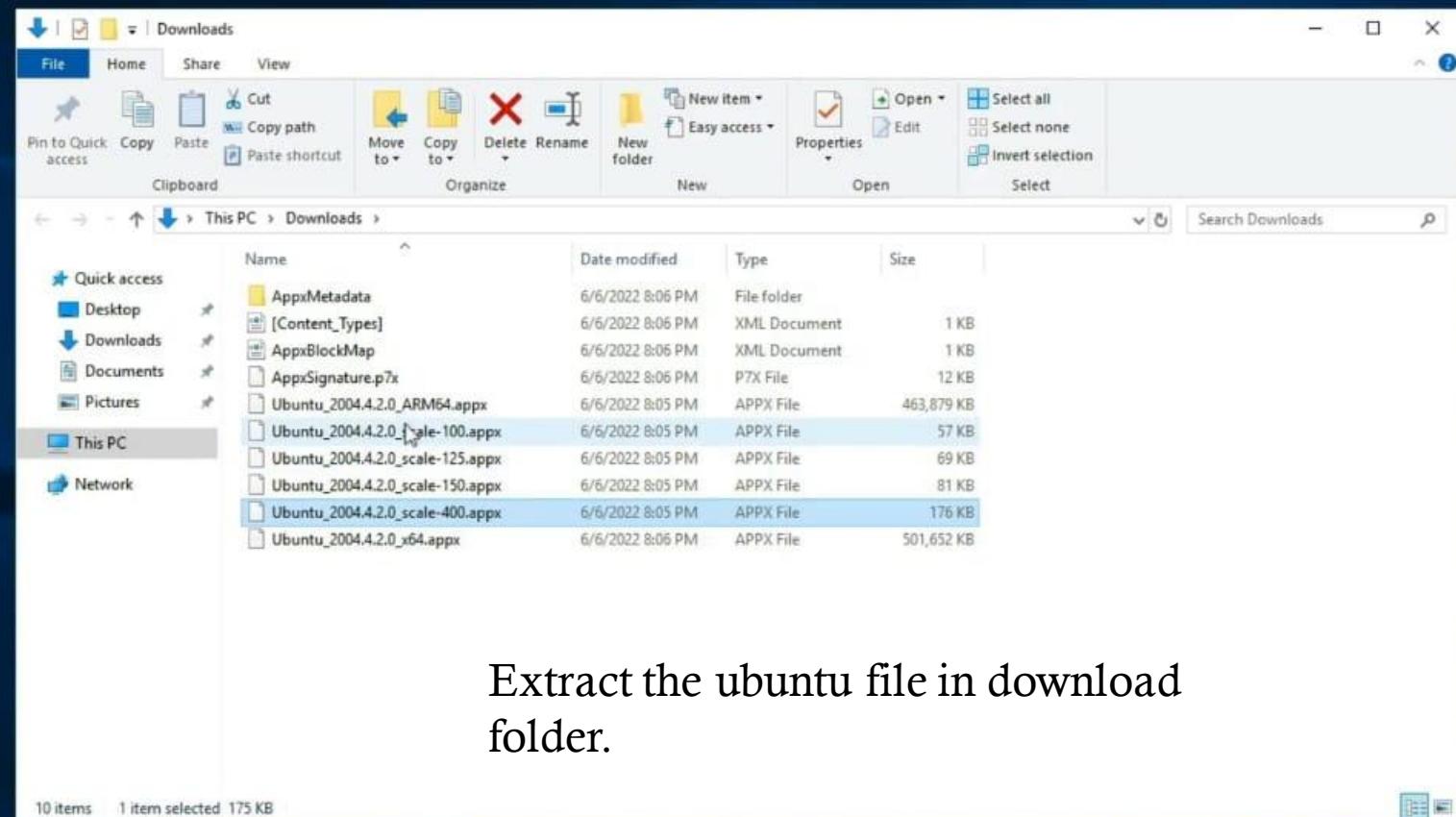
Administrator: Windows PowerShell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
PS C:\Users\Administrator> Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux

Run this command in power shell on server 2019.



Ubuntu file convert zip file.



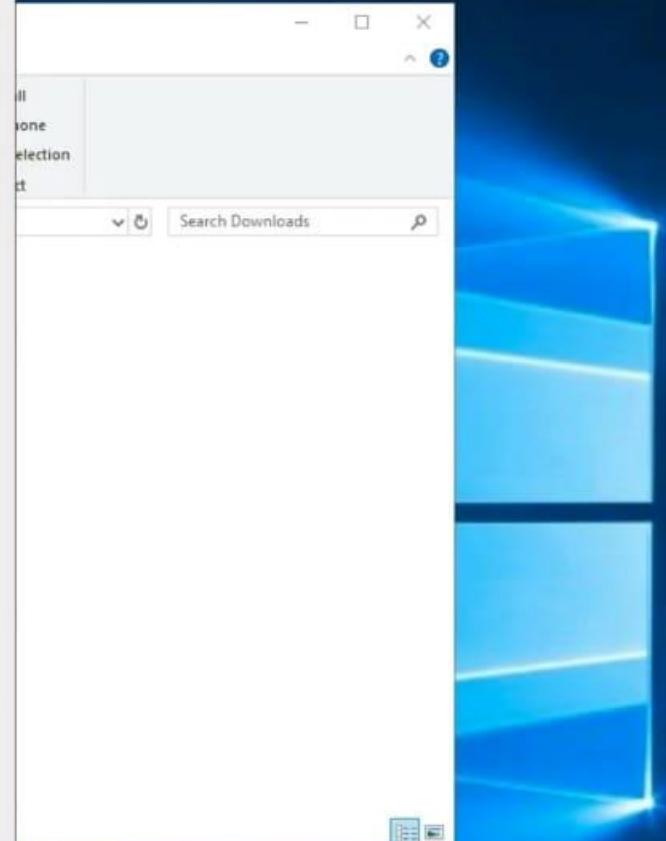


```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Downloads> dir

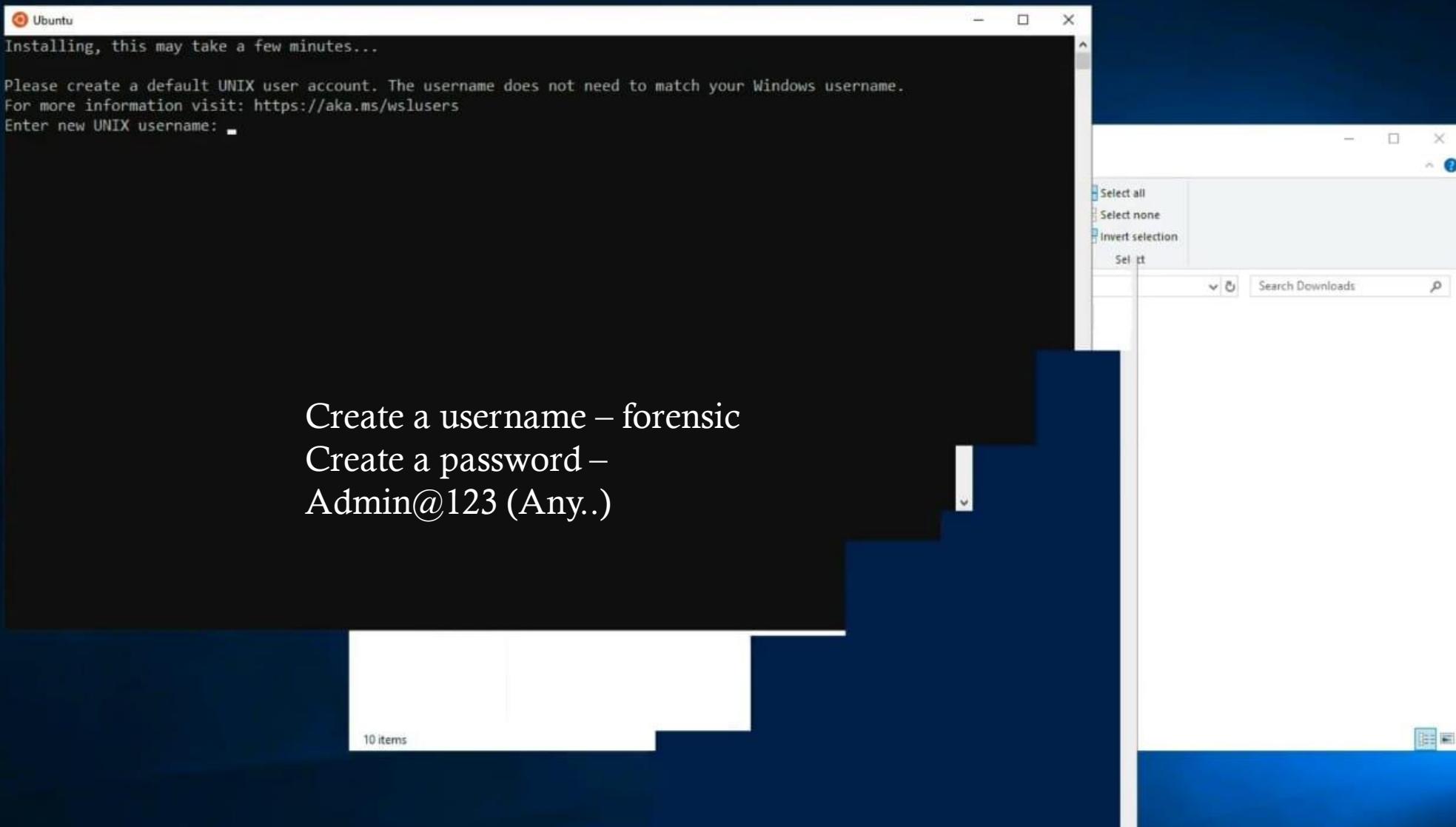
Directory: C:\Users\Administrator\Downloads

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.



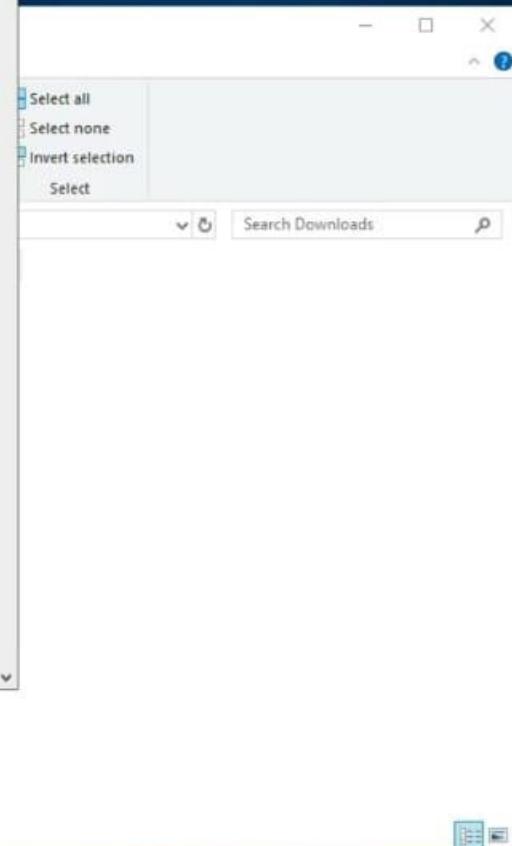
Create a username – forensic

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



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

Wish list



EVERYONE

Overview

System Requirements

Reviews

Related

### Available on



### 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

Windows 10 Enterprise Evaluation  
Windows Licence valid for 90 days



Home Gaming Entertainment Productivity Deals

### 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

Windows 10 Enterprise Evaluation  
Windows Licence valid for 90 days

## **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.

Installl the setup of Event log and Notepad++.

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

VirtualBox VM Machine View Input Devices Windows Help

Windows2019-FOR (Initial install) [Running]

Recycle Bin

Firefox

Event Log Explorer

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 AircacheParser.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 EZV1ewer.zip (Size: 73,114,127)

Downloaded hasher.zip (Size: 51,299,411)

Downloaded JLLCmd.zip (Size: 4,160,098)

Downloaded JumpListExplorer.zip (Size: 36,040,986)

Downloaded LECmd.zip (Size: 4,571,359)

Downloaded MFTExplorers.zip (Size: 4,214,450)

Downloaded MFTExplorers.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 ria.zip (Size: 4,126,404)

Downloaded SDBExplorer.zip (Size: 64,787,575)

Downloaded SBEcmd.zip (Size: 4,486,617)

Downloaded ShellBagsExplorer.zip (Size: 77,989,497)

Downloaded srLECmd.zip (Size: 6,838,917)

Downloaded SrumCmd.zip (Size: 4,365,882)

Downloaded SuntCmd.zip (Size: 3,603,159)

Downloaded TimelineExplorer.zip (Size: 63,456,641)

Downloaded VSDMount.zip (Size: 3,177,299)

Downloaded WICCmd.zip (Size: 4,141,090)

Downloaded ZistGeolocate.zip (Size: 38,438,180)

Downloaded TimeApp.zip (Size: 182,347)

Downloaded XWFIM.zip (Size: 62,759,806)

Downloaded ChangeLog.txt (Size: 31,572)

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

PS C:\Tools\EZTools>

File Explorer

Using this command  
all tool install in Eric  
Zimmerman tool

File		Home	Share	View	Manage	SDT_x64FREE_EN-US_VHD (C:)	—	□	X
		Drive Tools							
← → ↑ ↓		This PC > SDT_x64FREE_EN-US_VHD (C:)		▼ ▶		Search SDT_x64FREE_EN-US_V...	?		
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 (\\\VirtualBox\Shared F		>  Network			
8 items									
Windows		Search		File Explorer		Internet Explorer	Mozilla Firefox	05:33 09-07-2023	

Name

Date modified

Type

Size

Cases

30-06-2023 09:12

File folder

PerfLogs

15-09-2018 07:19

File folder

Program Files

07-07-2023 07:52

File folder

Program Files (x86)

28-06-2023 13:23

File folder

ProgramData

29-06-2023 16:46

File folder

Tools

28-06-2023 13:25

File folder

Users

27-06-2023 16:59

File folder

Windows

29-06-2023 21:43

File folder

File Home Share View

← → ↑ This PC > SDT\_x64FREE\_EN-US\_VHD (C:) > Tools >

Search Tools

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 (\\\) Network

Name Date modified Type Size

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	
kapec	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
kapec	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

10 items

05:35 09-07-2023

8. Install the windows 10 Enterprise version as a Target Sysytem 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.

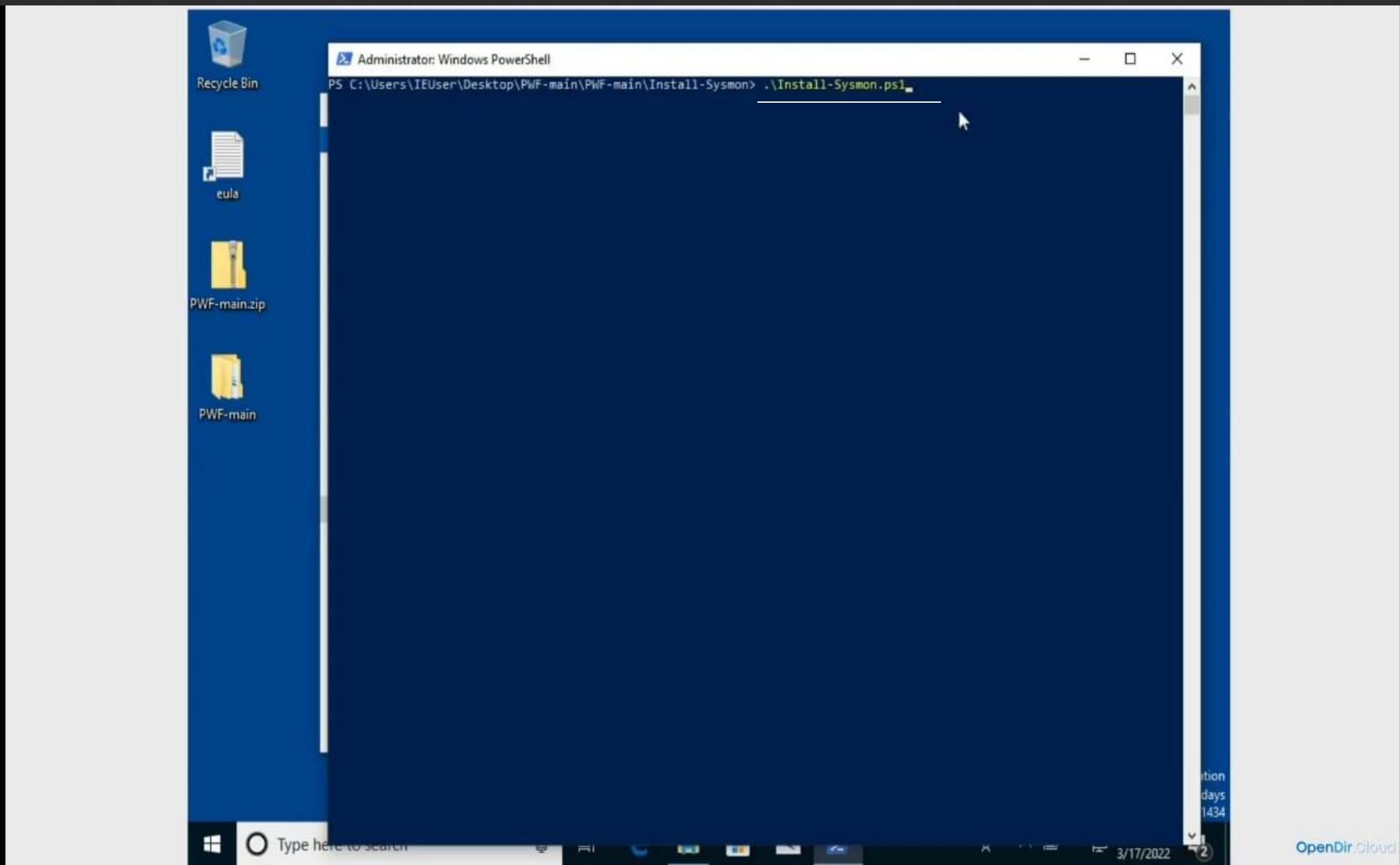
Attack Script Preparation- Go to the url <https://github.com/bluecapesecurity/PWF> zip file download and extract file.

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" running on a Windows 10 desktop. The command ".\ART-attack.ps1" is being executed from the path "C:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam". The script is performing several tasks:

- Installing the "Invoke-AtomicRedTeam" module.
- Running Atomic Tests, specifically T1566.001 and T1078.003, which involve downloading macro-enabled phishing attachments and creating local accounts with admin privileges.
- Executing PowerShell Fileless Script Execution tests, specifically T1059.001 and T1547.001, which involve running PowerShell scripts.
- Reg Key Run tests, specifically T1547.001-1, which involve modifying registry keys.

The PowerShell window also displays a progress bar and a message asking if the user wants to install the NuGet provider. The taskbar at the bottom shows other open applications like File Explorer, Edge, and Mail, along with system icons for battery, signal, and network.

```
Administrator: Windows PowerShell
PS C:\Users\IEUser\Desktop\PWF-main\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
PathToAtomsicsFolder = C:\AtomicRedTeam\atomsics

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
PathToAtomsicsFolder = C:\AtomicRedTeam\atomsics

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
PathToAtomsicsFolder = C:\AtomicRedTeam\atomsics

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
PathToAtomsicsFolder = C:\AtomicRedTeam\atomsics

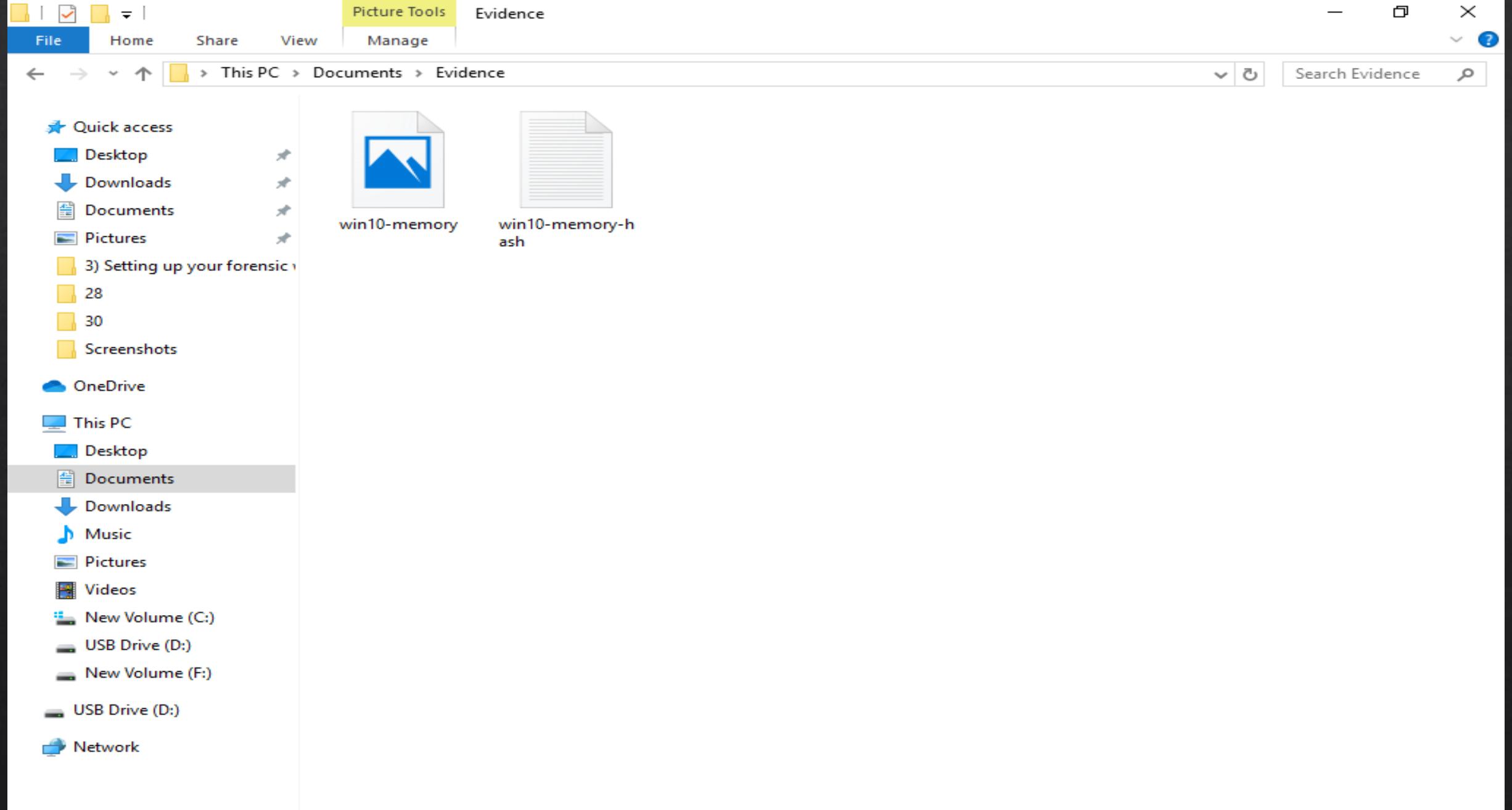
Using Logger: Default-ExecutionLogger
All logging commands found
Executing test: T1547.001-1 Reg Key Run
'
```

# 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.



2 items



Type here to search



14:14  
09-07-2023

## 10.Disk Acquisition target system

Oracle VM VirtualBox Manager

File Machine Medium Help

Tools

win2019-for (34 practical) Running

windows 10 (fresh installation) Powered Off

Target system (After attack shutdown) Powered Off

Add Create Copy Move Remove Release Search Properties Refresh

Hard disks Optical disks Floppy disks

Name	Virtual Size	Actual Size
{0926cce..._copy.vhd}	--	--
> 17763..._release_svc_refresh.190906-2324_server_datacenter...	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
> {abe...}.vdi	50.00 GB	9.42 GB
> {di...}	50.00 GB	1.36 GB
> {di...}	50.00 GB	50.00 GB

Copy... Ctrl+Shift+C  
Move... Ctrl+Shift+M  
Remove... Ctrl+Shift+R  
Release... Ctrl+Shift+L  
Search  
Properties

Attributes Information

Type: Normal

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

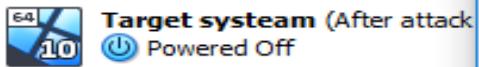
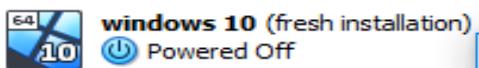
Apply Reset

Type here to search

11:54 09-07-2023



Tools



Hard disks

Optical disks

Floppy disks

Name

{0926cce4-dfd7-4e08-bd93-7a85bd797974}\_copy.vhd

Virtual Size

Actual Size

--

--

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

--

--

## 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

Type: Normal

Location: ers1\Denisha\VirtualBox VMs\Target system\Snapshots\{0e92291a-4319-4be6-8d4f-c9213ea20f88}.vdi

Description:

Size:

4.00 MB

50.00 GB

2.00 TB

Apply

Reset



Type here to search

11:54  
09-07-2023



Tools



win2019-for (34 practical)

Running



windows 10 (fresh installation)

Powered Off



Target system (After attack)

Powered Off

### 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

Type: Normal

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



Tools



win2019-for (34 practical)

Running



windows 10 (fresh installation)

Powered Off



Target system (After attack)

Powered Off

## Copy Virtual Disk

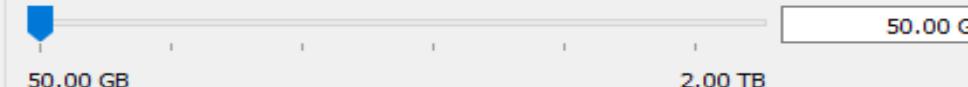


## Location and size of the disk image

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.

get system\VirtualBox VMs\Target system\Snapshots\{0e92291a-4319-4be6-8d4f-c9213ea20f88}\_copy.vhd

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.



Back

Finish

Cancel

Type: Normal

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



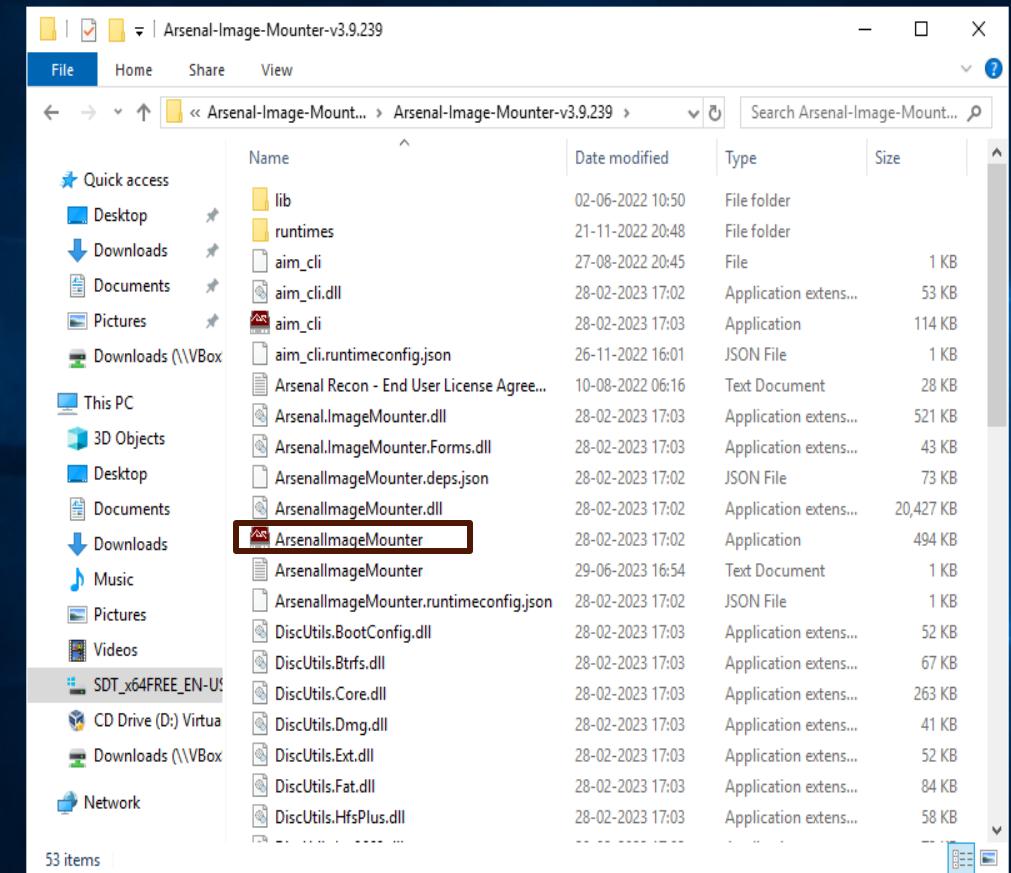
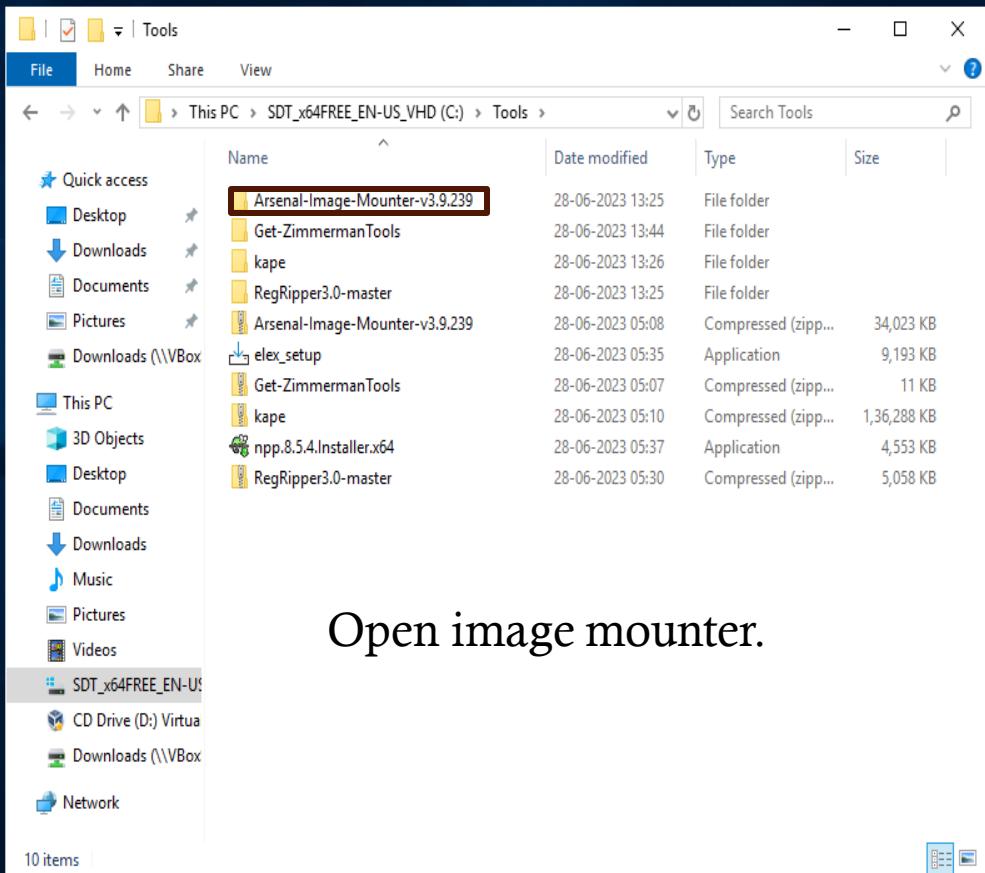
Type here to search

11:55  
09-07-2023

# Data Examination

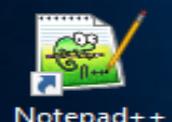
# Mounting the disk Image with Arsenal Image Mounter

You can enter the Target system harddisk





Recycle Bin



File 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 extent | 280 KB |

Size
53 KB
114 KB
1 KB
28 KB
521 KB
43 KB
73 KB
427 KB
494 KB
2 KB
1 KB
52 KB
67 KB
263 KB
41 KB
52 KB
84 KB
58 KB
73 KB
43 KB
90 KB





Recycle Bin

Arsenal Image Mounter

File BitLocker Advanced Help

No items found.

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

53 items | 1 item selected 493 KB | DiscUtil Ntfs.dll | 28-02-2023 17:04 | Application extent | 280 KB |

**ARSENAL RECON**

The screenshot shows the Arsenal Image Mounter application window. At the top, there's a toolbar with icons for file operations like 'Mount disk image', 'Mount VSCs', 'Launch VM', and 'Remove'. Below the toolbar is a large, empty list area with the message 'No items found.' In the bottom right corner of the window, there's a logo for 'ARSENAL RECON'. The taskbar at the bottom of the screen also displays the 'Arsenal Image Mounter' icon. The system tray in the bottom right corner shows the date and time as '29-06-2023 17:03'.

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

Mount image file

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-bd93-7a85b1...}

Supported formats

Open Cancel

Mount disk image Mount VSCs Launch VM Remove Remove all Refresh

53 items 1 item selected 493 KB

Diskfile Ntfc.dll

28-02-2023 17:04 Application extens

280 KB



ARSENAL RECON

Windows Server 2019 Datacenter Evaluation  
Windows License valid for 178 days  
Build 17763.rs5\_release.180914-1434

17:04  
29-06-2023





## Mount options

### 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

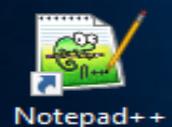
Windows License valid for 178 days  
Build 17763.rs5\_release.180914-1434

17:04  
29-06-2023





Recycle Bin



File Home Share View Manage Local Disk (F:)

← → ⌂ This PC > Local Disk (F:) >

Documents Pictures Downloads Evidence

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 (\\\VE Network

6 items

Name Date modified Type 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	

Search Local Disk (F:)

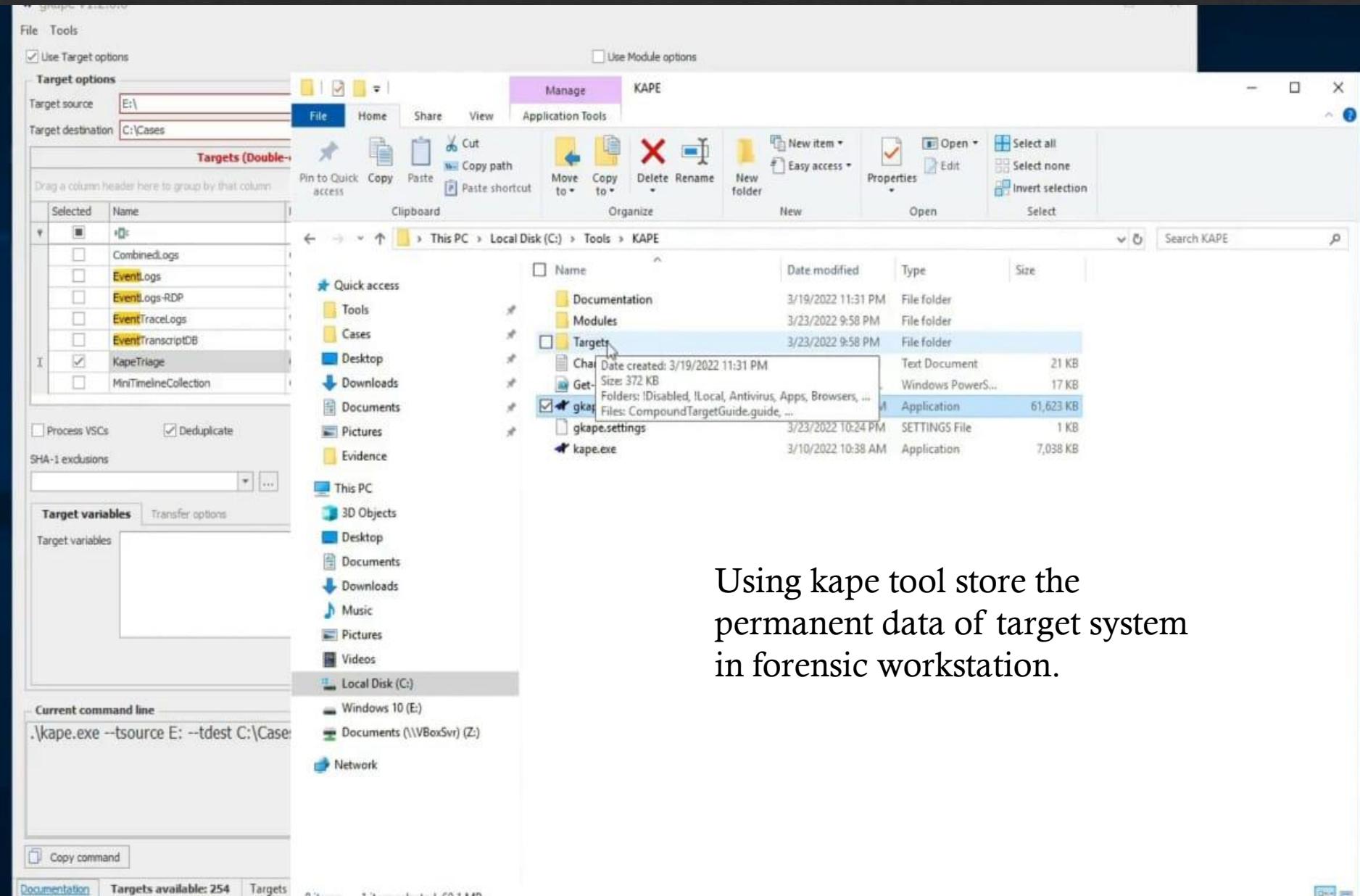
Show the hard disk of Target system in Forensic Workstation and you can show all data.

Windows Server 2019 Datacenter Evaluation  
Windows License valid for 178 days  
Build 17763.rs5\_release.180914-1434



17:08  
29-06-2023

# Creating a triage data collection with KAPE Tool



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

# All Data is store in Cases Folder.

The screenshot shows the Kape tool interface for collecting forensic data. The main window has two main sections: 'Targets' on the left and 'Modules' on the right.

**Targets (Double-click to edit a target)**

Selected	Name	Folder	Description
<input type="checkbox"/>	CombinedLogs	Compound	Collect Event logs, Trace logs, and more.
<input type="checkbox"/>	Event_logs	Windows	Event logs
<input type="checkbox"/>	Event_logs-RDP	Windows	Collect Win7+ RDP related logs
<input type="checkbox"/>	EventTraceLogs	Windows	Event Trace Logs
<input type="checkbox"/>	EventTranscriptDB	Windows	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 Firefox, etc), File History, Task History, Remote access software logs, 3rd party antivirus software logs, Windows 10 Timeline database, and \$1 Recycle Bin data files.
<input checked="" type="checkbox"/>	KapeTriage	Compound	Kape Triage
<input type="checkbox"/>	MinimelineCollection	Compound	Minimeline Collection

**Module options**

Selected	Name	Folder	Category	Description
<input type="checkbox"/>	IToolSync	Compound	Sync	Sync for new Maps, E...
<input type="checkbox"/>	EDParser	Compound	Modules	Eric Zimmerman Parser
<input type="checkbox"/>	AmcacheParser	EZTools	ProgramExecution	AmcacheParser extract
<input type="checkbox"/>	AppCompatCacheParser	EZTools	ProgramExecution	AppCompatCacheParser

**Current command line:**

```
.\cape.exe --tsource E: --tdest C:\Cases --tflush --gui
```

Bottom status bar:

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

File Tools

Use Target options

Use Module options

**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 logs
<input type="checkbox"/>	EventLogs	Windows	Event logs
<input type="checkbox"/>	EventLogs-RDP	Windows	Collect Win7+ RDP related logs
<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

**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"/>	IToolsSync	Compound	Sync	Sync for new Macro, B...
<input type="checkbox"/>	EDParser	Compound	Modules	Eric Zimmerman Parser
<input type="checkbox"/>	AntcacheParser	EZTools	ProgramExecution	AntcacheParser: extr...
<input type="checkbox"/>	AppCompatCacheParser	EZTools	ProgramExecution	AppCompatCachePar...
<input type="checkbox"/>	Remote Access	BMC-Tools: RDP Bitm...		
<input type="checkbox"/>	Modules	Run all existing Modul...		
<input type="checkbox"/>	KeywordSearches	Use listings to GREP		
<input type="checkbox"/>	CurrentSearches	Use listings in GREP		

Key   
Value

**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.

**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
```

Copy command

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



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\\$UsnJrn1:\$J' due to NotSupportedException...  
Deferring 'E:\\$Extend\\$UsnJrn1:\$Max' due to NotSupportedException...  
Deferring 'E:\\$Secure:\$SDS' due to NotSupportedException...  
Deferring 'E:\\$Boot' due to UnauthorizedAccessException...  
Deferring 'E:\\$Extend\\$RmMetadata\\$TxfLog\\$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\\$UsnJrn1:\$J' to 'C:\Cases\E\\$\\$Extend\\$J'. Hashing source file...  
Copied deferred file 'E:\\$Extend\\$UsnJrn1:\$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\\$TxfLog\\$Tops:\$T' to 'C:\Cases\E\\$\\$Extend\\$RmMetadata\\$TxfLog\\$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

Target variables

Key	Value

Add

Other options

Debug messages    Trace messages    Ignore FTK warning  
 Zip password    Retain local copies

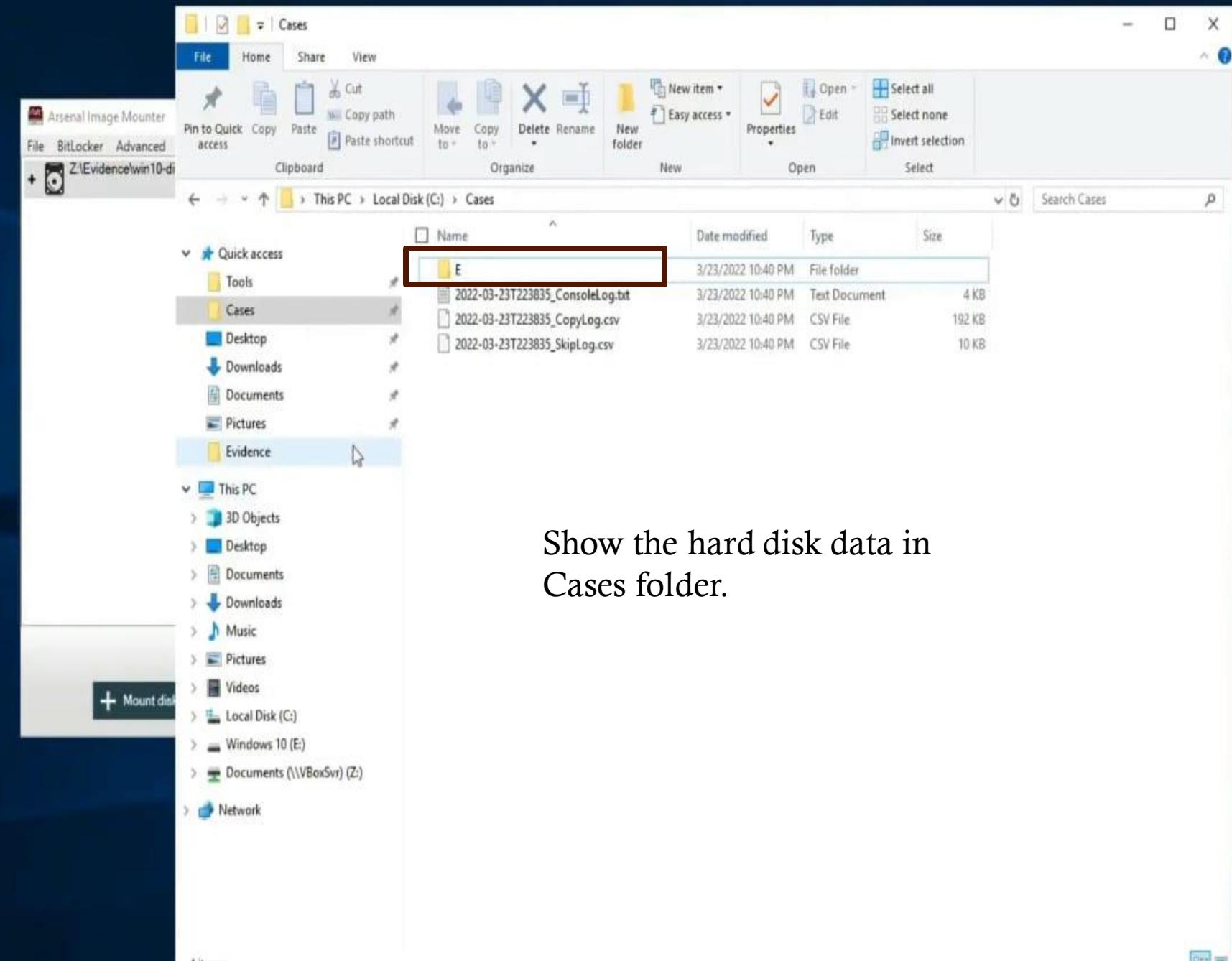
Current command line

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

Copy command Sync with GitHub Execute

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







Recycle Bin



Firefox



Notepad++

Event Log  
Explorer

Windows 10 (E)

File Home Share View Drive Tools Manage

Pin Cut Copy Paste Copy path Move to Copy Delete Rename New folder New item Open Easy access Properties Select all Open Select none Invert selection

Clipboard Organize New Open Select

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	

Quick access

- Tools
- Cases
- Desktop
- Downloads
- Documents
- Pictures
- Evidence

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C:)
- Windows 10 (E) **Selected**
- Documents (\\\VBoxSrv) (Z:)
- Network

+ Mount disk

8 items



# Disk Analysis Process

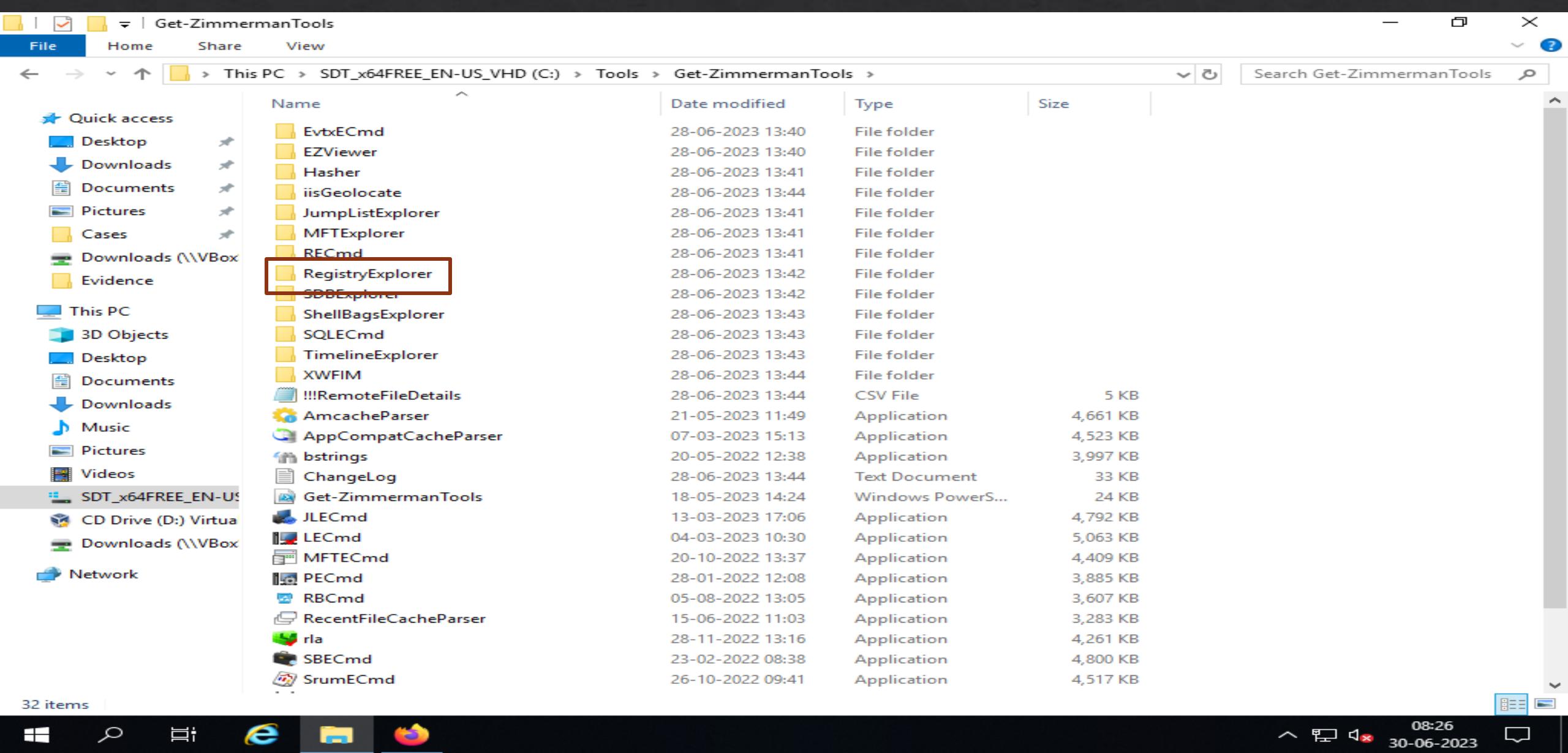
Go to the link and Download the materials.

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

# Windows Registry

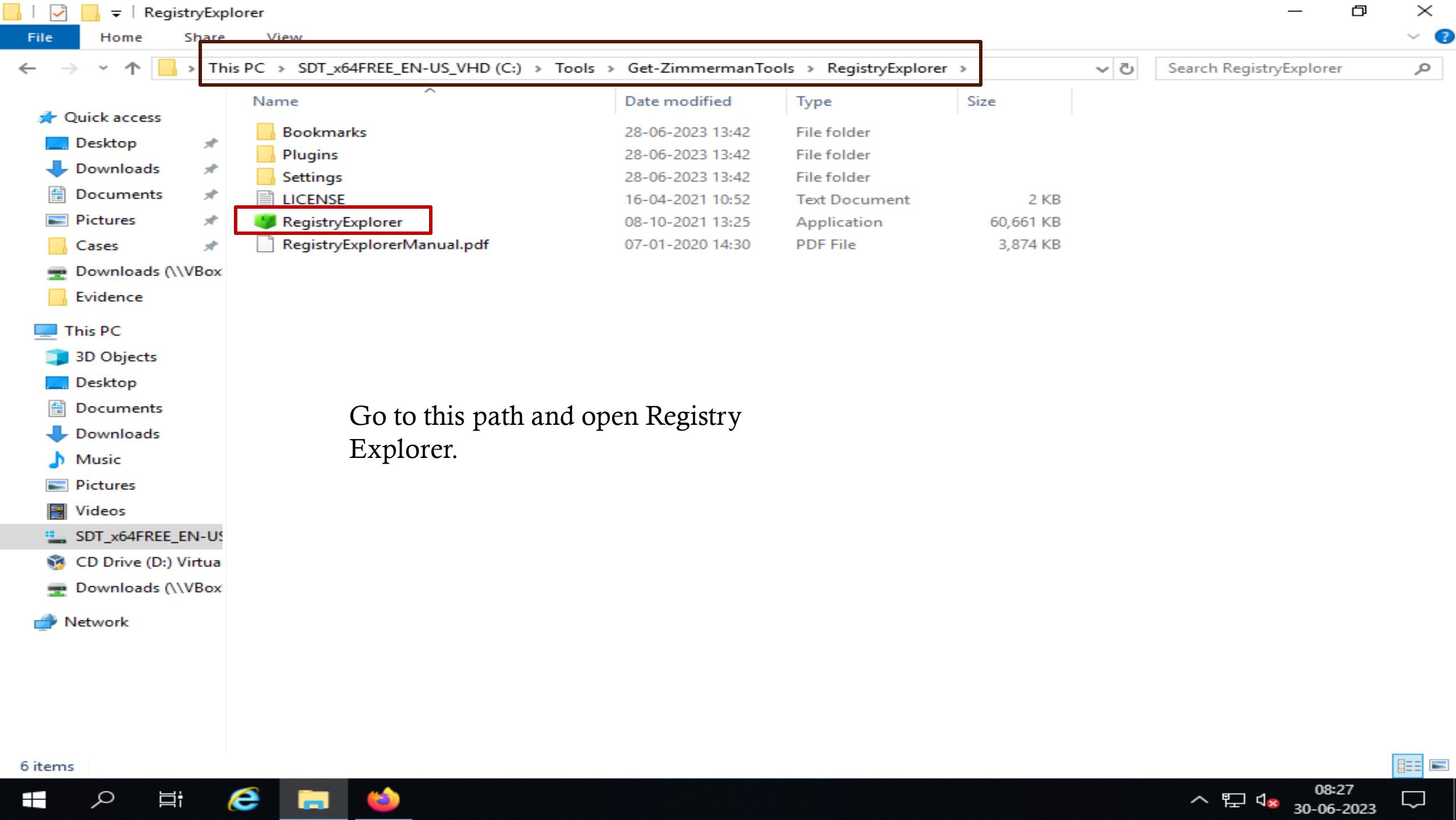
The **registry** or **Windows registry** is a database of information, settings, options, and other values for software and hardware installed on all versions of Microsoft Windows operating systems. When a program is installed, a new subkey is created in the registry. This subkey contains settings specific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

# Registry Explorer with Eric Zimmerman Tools

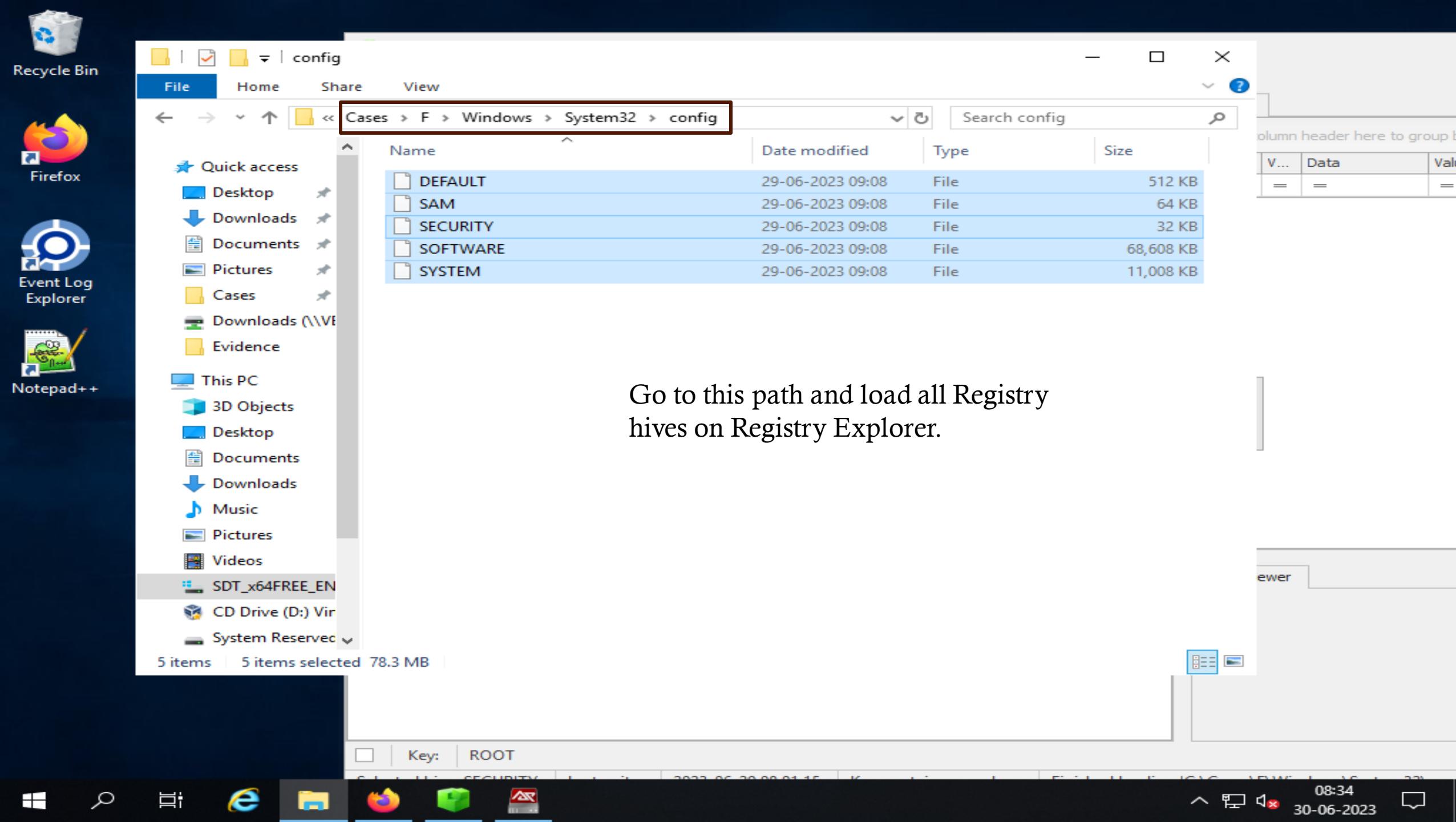


The screenshot shows a Windows File Explorer window with the following details:

- Path:** This PC > SDT\_x64FREE\_EN-US\_VHD (C:) > Tools > Get-ZimmermanTools
- File Explorer View:** Details
- Selected Item:** RegistryExplorer (highlighted with a red box)
- Items in the 'Get-ZimmermanTools' folder:** 32 items
- Table Headers:** Name, Date modified, Type, Size
- Items List:** EvtxECmd, EZViewer, Hasher, iisGeolocate, JumpListExplorer, MFTExplorer, RECmd, RegistryExplorer, SDBExplorer, ShellBagsExplorer, SQLECmd, TimelineExplorer, XWFIM, !!!RemoteFileDetails, AmcacheParser, AppCompatCacheParser, bstrings, ChangeLog, Get-ZimmermanTools, JLECmd, LECmd, MFTECmd, PECmd, RBCmd, RecentFileCacheParser, rla, SBECmd, SrumECmd



Go to this path and open Registry Explorer.



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
C:\Cases\F\Windows\System32\config\SEC...	=	=	=
ROOT	0	3	2023-06-29 08:01:15
C:\Cases\F\Windows\System32\config\DEF...	0	9	2023-06-29 08:27:03
ROOT	0	0	
Associated deleted records	0	0	
Unassociated deleted values	2	0	
C:\Cases\F\Windows\System32\config\SAM	0	1	2023-06-28 16:04:43
ROOT	0	0	
Associated deleted records	0	0	
C:\Cases\F\Windows\System32\config\SY...	0	17	2023-06-29 08:00:59
ROOT	0	0	
Associated deleted records	0	0	
Unassociated deleted records	0	0	
Unassociated deleted values	146	0	
C:\Cases\F\Windows\System32\config\SO...	0	17	2023-06-29 08:14:27
ROOT	0	0	
Associated deleted records	0	0	
Unassociated deleted records	0	0	
Unassociated deleted values	46	0	

Values

Drag a column header here to group by that column

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

Type viewer

Key: ROOT

Selected hive: SECURITY Last write: 2023-06-29 08:01:15 Key contains no values Load complete Value: None Hidden

Build 17763.rs5\_release.180914-1434

08:35 30-06-2023

**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

RBC

- ▶ 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
  - ▶ Channels
  - ▶ command
  - ▶ Control Panel
  - ▶ CurrentVersion
  - ▶ CurrentVersion
  - ▶ Windows Defender
  - ▶ Windows Defender
  - ▶ Devices

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:

Key: Microsoft\Windows\CurrentVersion

Selected hive: SECURITY Last write: 28-06-2023 17:12:44 +00:00 11 of 11 values shown (100.00%) Hidden keys: 0 1

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value...	Is Del...	Data Rec...
RBC	RegSz	C:\Pr...	00-00	<input type="checkbox"/>	<input type="checkbox"/>
ProgramFilesDir	RegSz	C:\Pr...		<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

08:39 30-06-2023

**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

R E C

- ▶ 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

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

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

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value ...	Is Del...	Data Re...
R E C	RegSz	R E C	R E C	<input type="checkbox"/>	<input type="checkbox"/>
(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

Key: ControlSet001\Control\ComputerName\ComputerName Value: ComputerName Collapse all hives

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

08:51 30-06-2023

# Gathering system information with RegRipper

## Follow the Step for Regripper

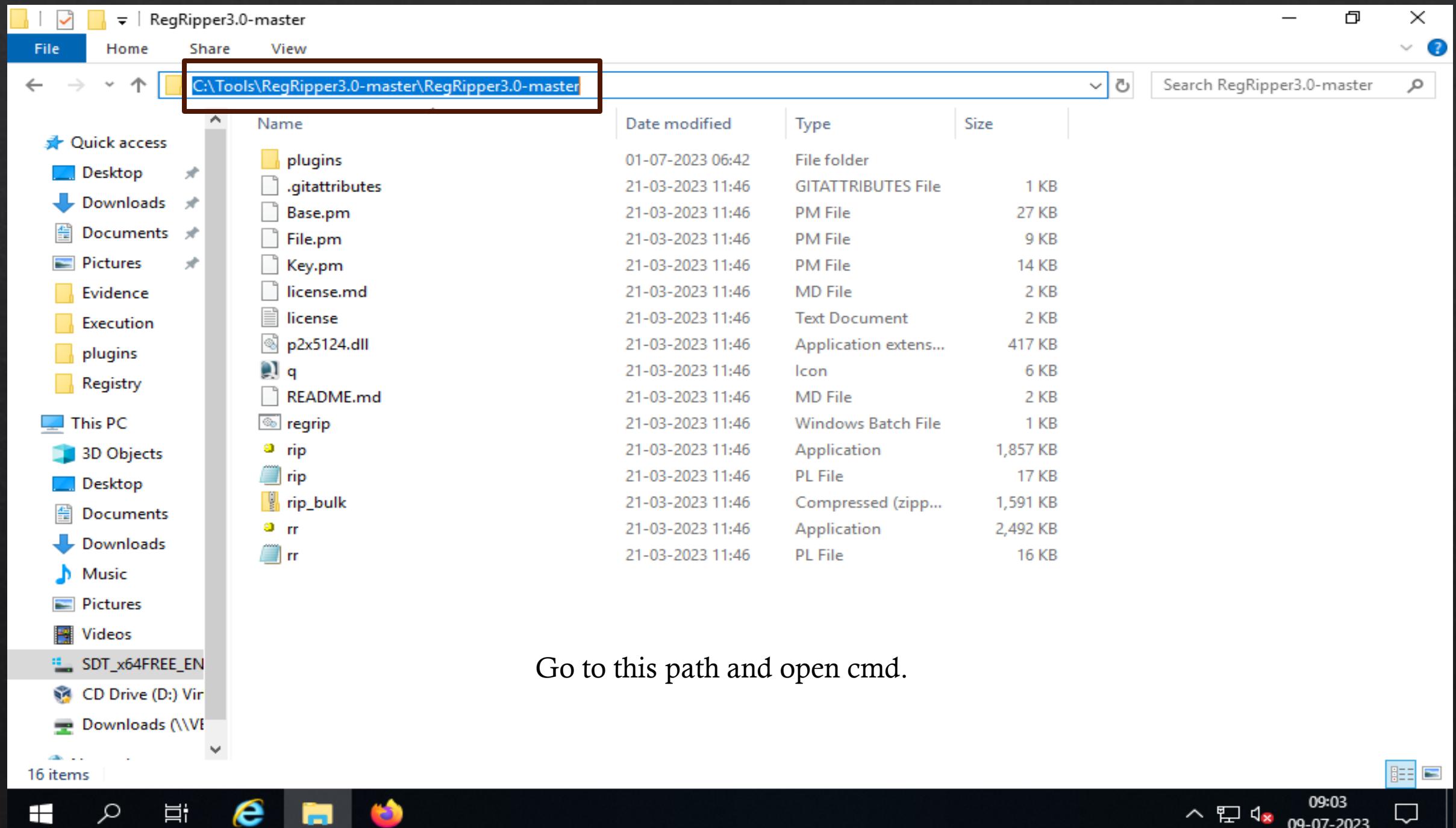
1. Go to the C:\Tools\RegRipper\ > open cmd > dir > rip.exe
2. You can create a folder in c drive with Analysis and also create registry folder in Analysis
3. Insert the file in Analysis folder:

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



RegRipper3.0-master

File Home Share View

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  
-d ..... Check to see if the hive is dirty  
-g ..... Guess the hive file type  
-a ..... Automatically run hive-specific plugins  
-aT ..... Automatically run hive-specific TLN plugins  
-f [profile].....use the profile  
-p [plugin].....use the plugin  
-l ..... list all plugins  
-c ..... Output plugin list in CSV format (use with -l)  
-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

Downloads (\\\WE)

16 items

09:16 09-07-2023

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

```
-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.



09:20  
09-07-2023

```
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 -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

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
```

Timezone plugin use for detail about time.

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.

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

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

14 items



09:39  
09-07-2023

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

Quick access

- 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)

14 items

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

Show the all text file of registry hives.

09:36 09-07-2023

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
SOFTW	01-07-2023 10:55	Text Document	2,476 KB
SOFTW	023 09:08	File	68,608 KB
SECUR	023 10:55	Text Document	4 KB
SECUR	023 09:08	File	32 KB
SAM	023 10:55	Text Document	8 KB
SAM	023 09:08	File	64 KB
NTUSE	023 11:02	Text Document	39 KB
NTUSE	023 09:07	DAT File	1,024 KB
DEFAU	023 10:55	Text Document	16 KB
DEFAU	023 09:08	File	512 KB

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

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

14 items | 1 item selected 2.41 MB



09:43  
09-07-2023

C:\Cases\Analysis\Registry\SYSTEM.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

2762 Name = vmicrdv  
2763 Display = @%systemroot%\system32\icsvcext.dll,-601  
2764 ImagePath = %systemroot%\system32\svchost.exe -k ICSservice -p  
2765 Type = Share  
2766 Start = Manual  
2767 Group =  
2768  
2769 Name = vmicsb  
2770 Display = @%syst  
2771 ImagePath = %syste  
2772 Type = Share\_  
2773 Start = Manual  
2774 Group =  
2775  
2776 Name = vmiicti  
2777 Display = @%syst  
2778 ImagePath = %syste  
2779 Type = Share\_  
2780 Start = Manual  
2781 Group =  
2782  
2783 Name = vmicvni  
2784 Display = @%syst  
2785 ImagePath = %syste  
2786 Type = Share\_

Find

Find Replace Find in Files Find in Projects Mark

Find what: shutdown

In selection

Find Next Count

Find All in Current Document

Find All in All Opened Documents

Close

Backward direction Match whole word only Match case Wrap around

Normal Extended (\n, \r, \t, \0, \x...) Regular expression

\_ matches newline

Transparency On losing focus Always

Normal text file length : 3,81,631 lines : 7,241 Ln : 2,788 Col : 15 Pos : 1,08,816 Windows (CR LF) UTF-8 INS

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\

100%

17:26 30-06-2023

Show any information using plugin.



all SYSTEM.txt DEFAULT.txt NTUSER.DAT.txt SAM.txt SECURITY.txt SOFTWARE.txt

```

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,,

```

Normal text file

length: 3,81,631 lines: 7,241

Ln: 2,788 Col: 15 Pos: 1,08,816

Windows (CR LF) UTF-8

INS

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 [REDACTED]
The syntax of this command is:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
HELPMSG | 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 [REDACTED]
User accounts for \\WIN-AJDB7GOIQUEJ
-----
Administrator          DefaultAccount          Guest
WDAGUtilityAccount
The command completed successfully.

C:\Users\Administrator>net localgroup [REDACTED]
Aliases for \\WIN-AJDB7GOIQUEJ
-----
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Certificate Service DCOM Access
*Cryptographic Operators
```



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

```
Aliases for \\WIN-AJDB7GOIQUEJ
```

```
-----  
*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-ajdb7goiquej\administrator
```

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

```
USER INFORMATION
```

```
-----
```

User Name	SID
Administrator	S-1-5-20-1000



\*Users

The command completed successfully.

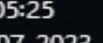
C:\Users\Administrator>whoami  
win-ajdb7goiqej\administrator

C:\Users\Administrator>whoami /user

USER INFORMATION

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

C:\Users\Administrator>



05:25  
01-07-2023

# Analysis of user accounts , groups and profiles

All Hives load in Registry Explorer and open SAM hive and click the on the user folder.

The screenshot shows the Registry Explorer interface with the following details:

- File menu:** File, Tools, Options, Bookmarks (0/0), View, Help.
- Toolbar:** Registry hives (5), Available bookmarks (73/0).
- Search Bar:** Enter text to search... with a Find button.
- Left pane (Tree View):** Key name, RBC filter, expanded to show C:\Cases\Analysis\Registry\DEFAULT, C:\Cases\Analysis\Registry\SAM (selected), Aliases, Users, C:\Cases\Analysis\Registry\SECURITY, C:\Cases\Analysis\Registry\SYSTEM, and C:\Cases\Analysis\Registry\SOFTWARE.
- Bookmark Information:** Hive: C:\Cases\Analysis\Registry\SAM, Category: Operating system, Name: Users, Key path: SAM\Domains\Account\Users, Short description: User accounts, Long description: User accounts in SAM file.
- Right pane (Table View):** Values tab selected, showing user accounts. The table has columns: ... (checkbox), 0 (Index), 4 (Value name), ..., Denisha (Value type), Adm (Data), and a column of checkboxes. Two rows are visible:
  - Row 1: Value name is "Denisha", Value type is "RegDword".
  - Row 2: Value name is "default user 0", Value type is "RegDword".
- Bottom Status Bar:** Key: SAM\Domains\Account\Users, Selected hive: DEFAULT, Last write: 28-06-2023 16:32:29 +00:00, 1 of 1 values shown (100.00%), Value: (default), Hidden keys: 0 1, 05:48, 01-07-2023.

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (0/0) View Help

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

Enter text to search... Find

Key name

ABC

- C:\Cases\Analysis\Registry\DEFAULT
- C:\Cases\Analysis\Registry\SAM
  - Aliases
  - Users
- C:\Cases\Analysis\Regis
- C:\Cases\Analysis\Regis
- C:\Cases\Analysis\Regis

Bookmark information

Hive C:\Cases\

Category Operating system

Name Users

Key path SAM\Domains\Account\Users

Short description User accounts

Long description User accounts in SAM file

Key: SAM\Domains\Account\Users Value: (default) Value: (default) Collapsible all hives

Selected hive: DEFAULT Last write: 28-06-2023 16:32:29 +00:00 1 of 1 values shown (100.00%) Hidden keys: 0 1

Values User accounts

Drag a column header here to group by that column

Den is ha Ad mi ni st ra to

{ ve rsi on "1, "que sti on s":[]}

Export successful

i Values exported to 'C:\Users\Administrator\Desktop\User accounts\_Values\_Export\_20230701054831.xlsx'

OK

Total rows: 6

Export ?

Type viewer

Value name (default)

Value type RegDword

0

05:48 01-07-2023 1

Desktop

File Home Share View

← → ⌂ ⌃ ⌄ This PC > Desktop Search Desktop

Quick access

- 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)

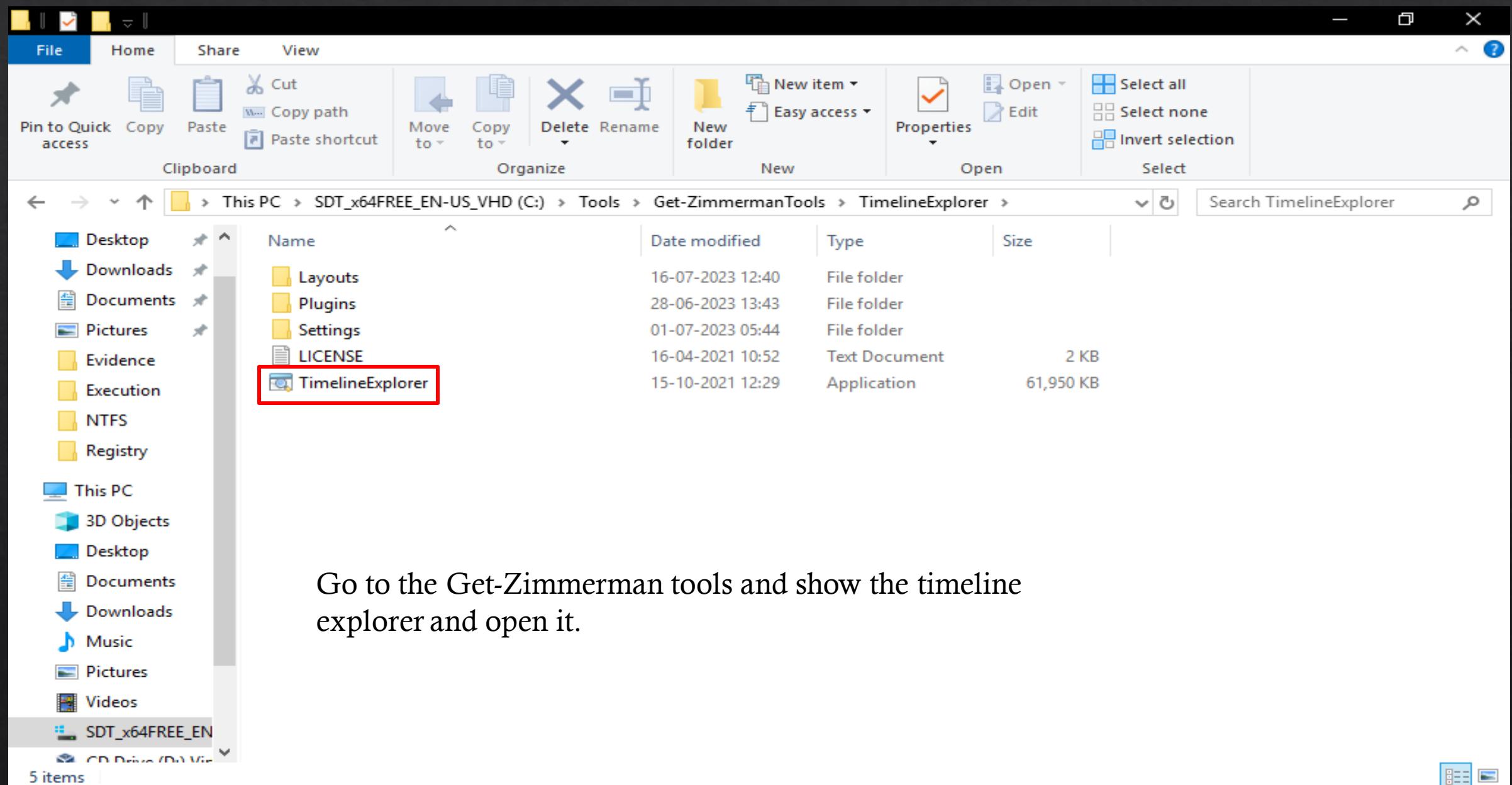
3 items

Name Date modified Type Size

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

Open this file in timeline explorer

10:04 09-07-2023



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



05:37  
02-08-2023





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

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
=	=	=	RBC	RBC	RBC
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.

File | 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

12 items | 1 item selected 7.09 KB

06:01 01-07-2023

SAM file open with notepad++



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
```

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.
```

RegistryExplorer

File Home Share View

C:\Tools\Get-ZimmermanTools\RegistryExplorer

Search RegistryExplorer

Quick access

- 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)

6 items

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

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

10:27 09-07-2023

# 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

RBC = ^

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

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...
RBC	RBC	RBC	RBC	=	=	=
RecentDocs	8	invoke-atomicredteam	invoke-atomicredteam (2).lnk	0	2023-06-28 ...	2023-06-28 1...
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

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

00000000 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 ?

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

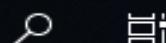
Value: MRUListEx Collapse all hives

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



10:19  
09-07-2023

# Open Ntuser.dat file in Notepad++.

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

```
726 Software\Microsoft\Windows\CurrentVersion\Search\RecentApps not found.  
727 -----  
728 recentdocs v.20200427  
(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.ps1  
740     6 = Resources  
741     5 = PracticalWindowsForensics-cheat-sheet.pdf  
-----
```

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\.ps1  
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
```

Normal text file length: 39,529 lines: 1,000 Ln: 728 Col: 11 Sel: 10 | 1 Windows (CR LF) ANSI INS

10:22 09-07-2023

# 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 DEFAULT.txt NTUSER.DAT.txt SECURITY.txt SOFTWARE.txt SAM.txt UsrClass.dat.txt SYSTEM.txt

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 [Deskt
133	2023-06-28 16:33:34	2023-06-28 16:33:32		99809/3	My Computer\CLSID_Desktop\PWF-mai
134	2023-06-28 16:33:36	2023-06-28 16:33:32		99812/2	My Computer\CLSID_Desktop\PWF-mai
135	2023-06-28 16:33:36	2023-06-28 16:33:36		99845/2	My Computer\CLSID_Desktop\PWF-mai
136	2023-06-28 16:33:36	2023-06-28 16:33:34		99830/3	My Computer\CLSID_Desktop\PWF-mai
137	2023-06-28 17:45:00	2023-06-28 17:45:00		99852/3	My Computer\CLSID_Desktop\PWF-mai
138	2023-06-28 16:33:36	2023-06-28 15:27:16			My Computer\CLSID_Desktop\PWF-mai
139			2023-04-27 13:32:14		My Computer\CLSID_Desktop\PWF-mai
140			2023-04-27 13:32:14		My Computer\CLSID_Desktop\PWF-mai
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 [Des
143	2023-06-28 17:57:04	2023-06-28 16:42:38		99737/4	My Computer\C:\AtomicRedTeam\invo
144	2023-06-28 17:57:04	2023-06-28 16:42:38		99868/3	My Computer\C:\AtomicRedTeam\invo
145	2023-06-28 17:57:04	2023-06-28 16:42:38		100972/4	My Computer\C:\AtomicRedTeam\invo
146	2023-06-28 17:57:16	2023-06-28 17:57:08		104667/10	My Computer\C:\AtomicRedTeam\atom
147	2023-06-29 08:01:18	2019-12-07 09:14:54		60/1	My Computer\C:\Program Files [Des
148	2023-06-29 08:09:56	2023-06-28 16:30:32		102703/2	My Computer\C:\Program Files\Orac
149	2023-06-29 08:09:50	2023-06-28 16:30:32		102704/2	My Computer\C:\Program Files\Orac
150	2023-06-29 08:01:18	2019-12-07 09:14:54		1223/1	My Computer\C:\Program Files (x86
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-Sys
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

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

11:01 09-07-2023

# 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 DEFAULT.txt NTUSER.DAT.txt SECURITY.txt SYSTEM.txt SOFTWARE.txt SAM.txt UsrClass.dat.txt

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

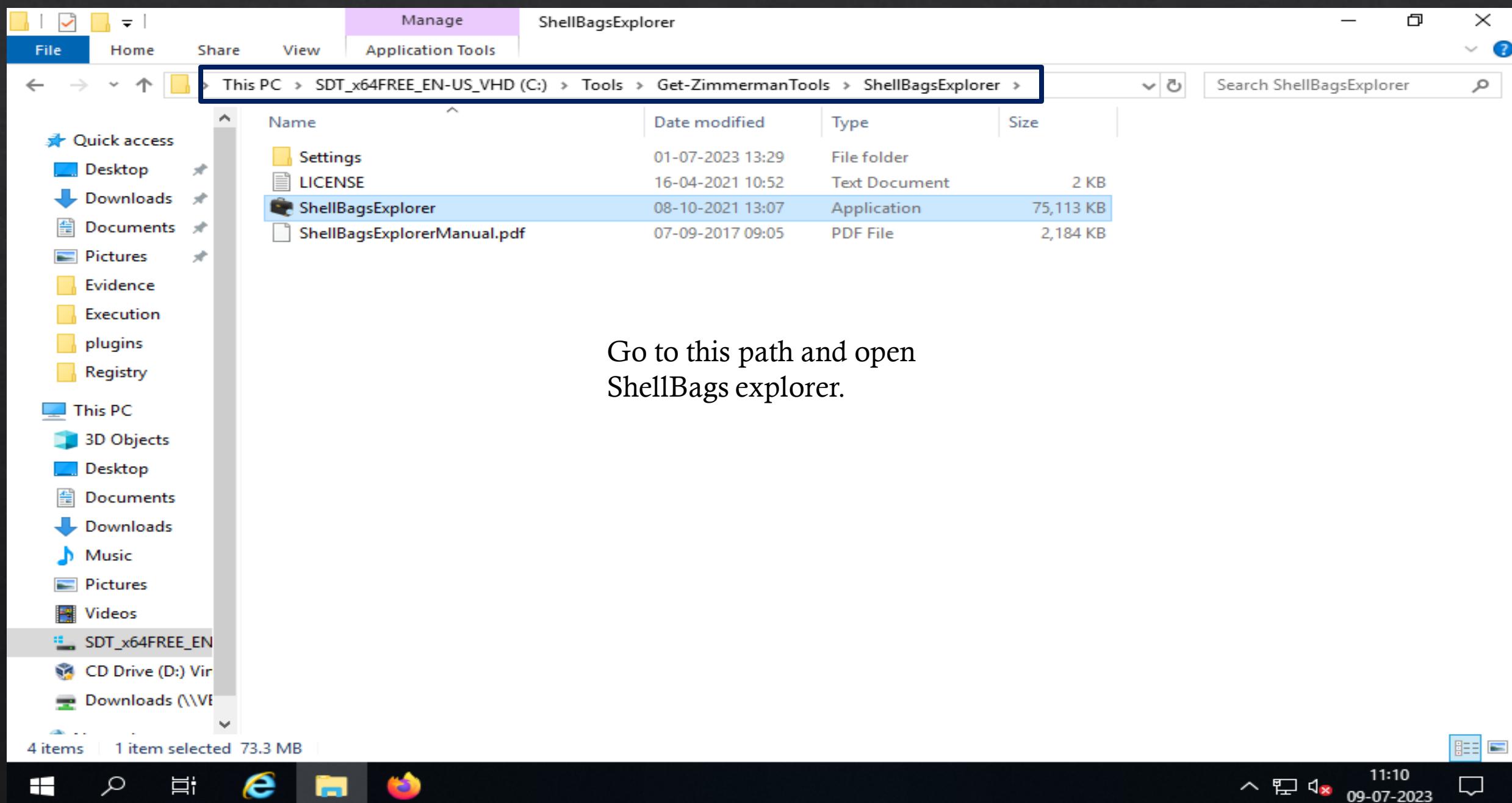
125

126 MRU Time	126  Modified	126 Accessed	126 Created	126 Zip_Subfolder	126 MFT
-----	-----	-----	-----	-----	-----
128 2023-06-29 08:12:06					
129 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
130 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
131 2023-06-28 16:33:44	2023-06-28 16:33:36	2023-06-28 16:33:36	2023-06-28 16:33:36		9984
132 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
133 2023-06-28 17:56:18	2023-06-28 17:45:00	2023-06-28 17:45:00	2023-06-28 17:45:00		9985
134 2023-06-28 17:56:18	2023-06-28 15:27:30	2023-06-28 16:33:36	2023-06-28 15:27:16		
135 2023-06-28 16:49:10				2023-04-27 13:32:14	
136 2023-06-28 16:49:53				2023-04-27 13:32:14	
137 2023-06-29 08:11:52					
138 2023-06-28 17:56:46	2023-06-28 17:56:46	2023-06-28 17:56:46	2023-06-28 16:42:32		9967
139 2023-06-28 16:42:38	2023-06-28 16:42:38	2023-06-28 17:57:04	2023-06-28 16:42:38		9973
140 2023-06-28 16:42:38	2023-06-28 16:42:38	2023-06-28 17:57:04	2023-06-28 16:42:38		9986
141 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
142 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
143 2023-06-28 16:30:32	2023-06-28 16:30:32	2023-06-29 08:01:18	2019-12-07 09:14:54		60/1
144 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
145 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
146 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
147 2023-06-28 15:27:30	2023-06-28 15:27:30	2023-06-28 16:33:22	2023-06-28 15:27:16		
148 2023-06-28 16:48:32				2023-04-27 13:32:14	
149 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



# Insert the UsrClass.dat

ShellBags Explorer v1.4.0.0

Select a registry hive to open. Hold SHIFT to ignore dirty Registry hives

Analysis > Registry

Organize New folder

Name Date modified Type

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

# ShellBags Explorer v1.4.0.0

File Tools Help

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
Home Folder	Root folder: GUID	Root folder: GUID	=	=	=	=
My Computer	Root folder: GUID	Root folder: GUID	0			
PWF-main.zip	File	File	3	2023-06-28 15:27:16	2023-06-28 15:27:30	2023-06-28 16:33:22
PWF-main	Directory	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

'UsrClass.dat' Registry hive loaded in 2.3714 seconds!

4 shellbags loaded in 0.0092 seconds

Time zone: UTC 4 of 4 rows visible (100.00%)

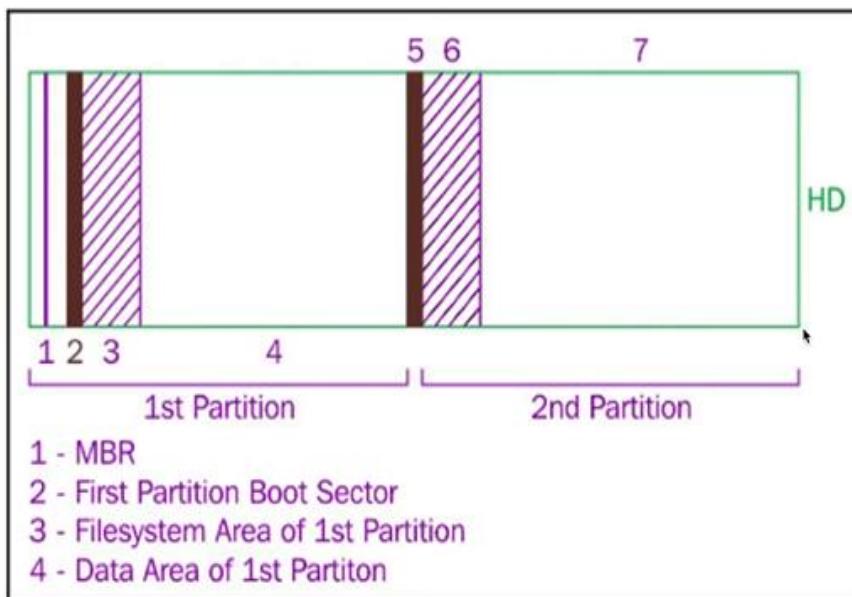


11:13  
09-07-2023

# 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



# 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:

- Toolbar:** Includes icons for 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.
- Address Bar:** Displays the path: This PC > SDT\_x64FREE\_EN-US\_VHD (C:) > Cases > F >.
- Left Navigation:** Shows a sidebar with links to Desktop, Downloads, Documents, Pictures, Cases, Evidence, Execution, Registry, This PC, 3D Objects, Desktop, Documents, Downloads, Music, Pictures, Videos, and SDT\_x64FREE\_EN. The SDT\_x64FREE\_EN link is highlighted.
- File List:** A table showing the contents of the 'F' 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
<b>SMFT</b>	29-06-2023 05:02	File	1,14,432 KB
\$Secure_SSOS	29-06-2023 05:02	File	2,007 KB
- Status Bar:** Shows 8 items | 1 item selected | 111 MB |
- System Tray:** Shows the date and time as 11:45 and 28-07-2023.

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

Manage

File Home Share View Application Tools

Pin to Quick access Copy Paste Cut Copy path Move to Copy to Delete Rename New folder New item Open Easy access Properties Select all Select none Invert selection

Clipboard Organize New Open Select

← → ↑ ↓ This PC > SDT\_x64FREE\_EN-US\_VHD (C:) > Tools > Get-ZimmermanTools Search Get-ZimmermanTools

Name	Date modified	Type	Size
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
RBCmd	05-08-2022 13:05	Application	3,607 KB

32 items 1 item selected 4.30 MB

Open the MFTExplorer in cmd.

File Explorer ribbon bar: File, Home, Share, View, Application Tools.

Clipboard section: Pin to Quick access, Copy, Paste, Cut, Copy path, Move to, Copy to, Delete, Rename, New folder, New item, Open, Easy access, Properties, Select all, Select none, Invert selection.

Organize section: Clipboard, New, Open, Select.

Address bar: This PC > SDT\_x64FREE\_EN-US\_VHD (C:) > Tools > Get-ZimmermanTools.

Search bar: Search Get-ZimmermanTools.

File Explorer sidebar: Desktop, Downloads, Documents, Pictures, Evidence, Execution, NTFS, Registry, This PC, 3D Objects, Desktop, Documents, Downloads, Music, Pictures, Videos, SDT\_x64FREE\_EN, CD Drive (D:\) VHD.

File Explorer status bar: 32 items, 1 item selected, 4.30 MB.

Taskbar icons: File Explorer, Edge, File Explorer, Firefox, Task View, Start button, Search icon, Task View icon, Volume icon, Battery icon, Network icon, 05:54, 02-08-2023, Notifications.

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



11:48  
28-07-2023

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

```
--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.ffffffff]
--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

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

```
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: 0x
0, 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.



12:02  
28-07-2023

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

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

```
c:\ 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.ffffffff]
--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

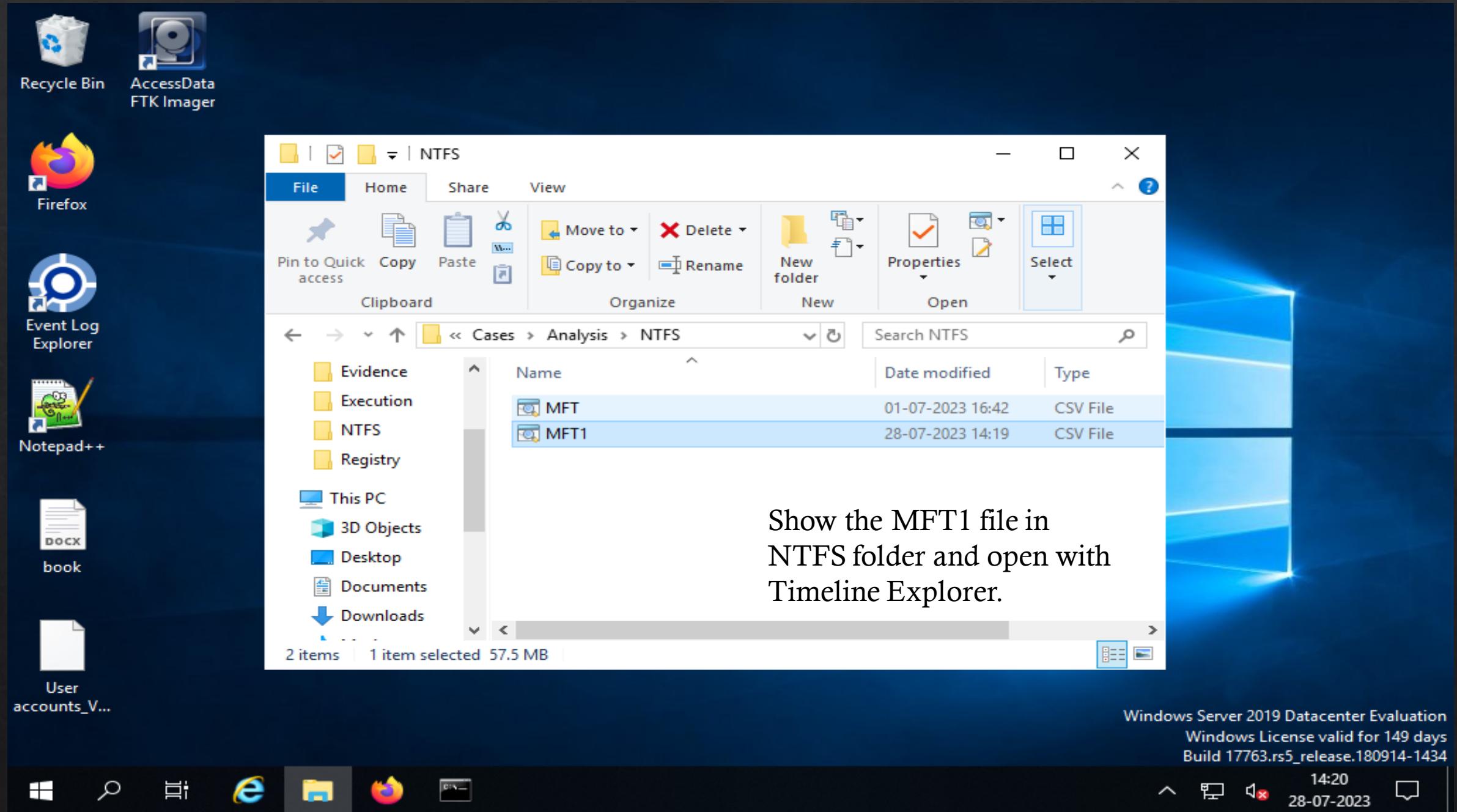
Processed c:\Cases\F\$MFT in 11.7887 seconds

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.



Drag a column header here to group by that column

PWF-main

x ▾

Find

.	In U...	Parent Path	File Name	Extensi...
T		RBC	RBC	RBC
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.

Drag a column header here to group by that column

PWF-main

x ▾

Find

	File Size	Created0x10	Created0x30	Last Modified0x10	Last Modified0x30	Last Record Change0x10
▼	=	=	=	=	=	=
	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 file with USN Journal analysis

The screenshot shows a Windows File Explorer window. The left sidebar contains a navigation tree with items like Evidence, Execution, NTFS, Registry, This PC, 3D Objects, Desktop, Documents, Downloads, Music, Pictures, Videos, SDT\_x64FREE\_EN, CD Drive (D:) Vir, Downloads (\\\), and Network. The main pane displays a list of files and folders under the path This PC > SDT\_x64FREE\_EN-US\_VHD (C:) > Cases > F. The list includes:

Name	Date modified	Type	Size
SExtend	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	
SBoot	30-06-2023 08:31	File	8 KB
SLogFile	30-06-2023 08:31	File	65,536 KB
SMFT	29-06-2023 05:02	File	1,14,432 KB
SSecure_SSFS	29-06-2023 05:02	File	2,007 KB

At the bottom right of the main pane, there is a text overlay: "Using this file for journaling part."

At the bottom of the screen, the taskbar shows icons for File Explorer, Edge browser, and File Explorer again. The system tray at the bottom right shows the date and time (06:02, 02-08-2023) and several notification icons.

File | Home | Share | View | Manage | Get-ZimmermanTools | Application Tools | - X

← → ↑ ↓ cmd Search for "cmd" Search Get-ZimmermanTools ?

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:) Local Disk (G:) Downloads (\\\VE Network

cmd

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
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
SQLECmd	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 4.30 MB

MFTCmd open

12:27 09-07-2023

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

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.ffffffff]
- 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

```
C:\> 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

NTFS1

File Home Share View

This PC > SDT\_x64FREE\_EN-US\_VHD (C:) > Cases > Analysis > NTFS1

Search NTFS1

Pictures Evidence Execution NTFS Registry This PC 3D Objects Desktop Documents Downloads Music Pictures Videos SDT\_x64FREE\_EN CD Drive (D:) Virtual System Reserved Local Disk (F:) Local Disk (G:) Downloads (\\\V) Network

Name Date modified Type Size

20230709123220\_MFTECmd\_SMFT\_Output 09-07-2023 12:32 CSV File 58,903 KB  
20230709123240\_MFTECmd\_SJ\_Output 09-07-2023 12:32 CSV File 50,449 KB

2 items | 1 item selected 49.2 MB

12:37 09-07-2023

Drag a column header here to group by that column

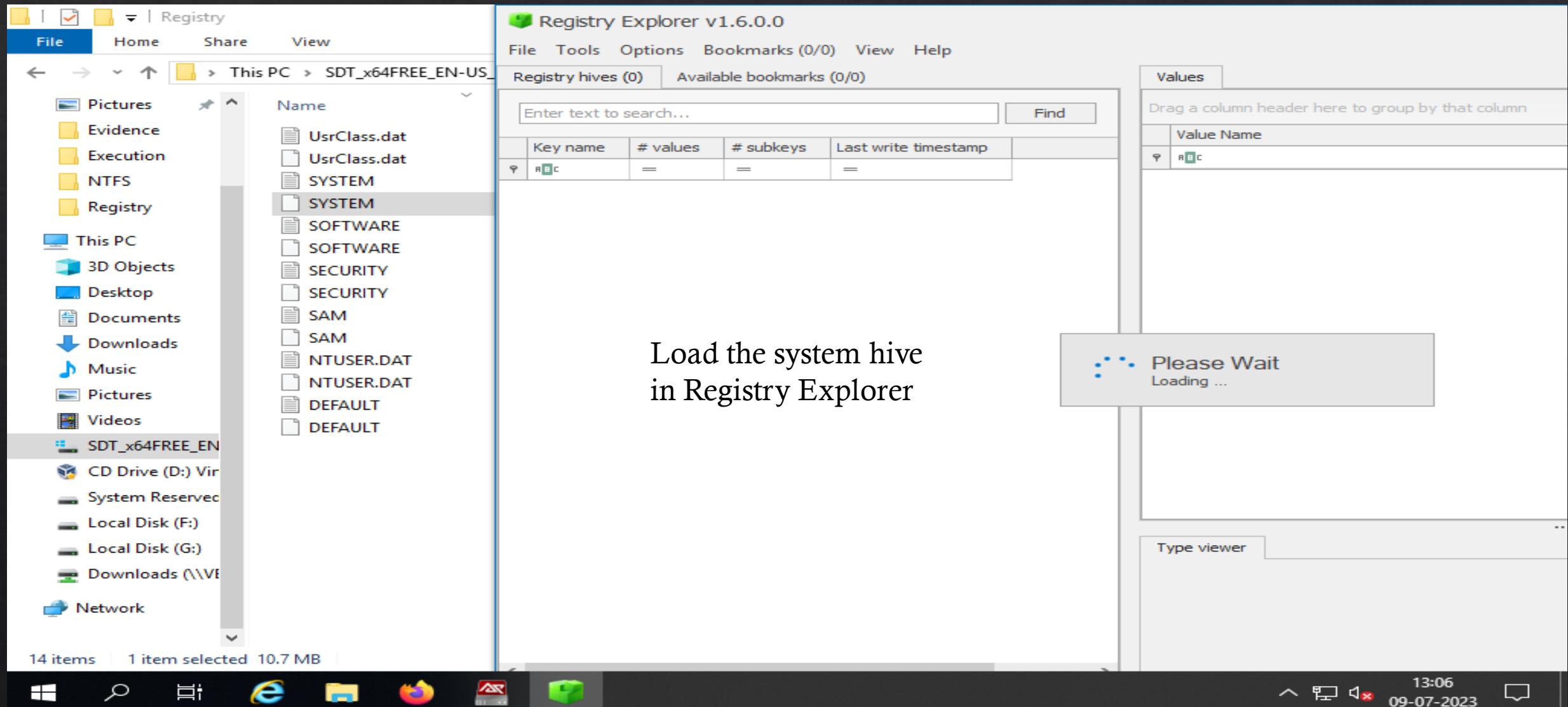
Enter text to search...

Find

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

# Evidence of Execution

## 1. BAM ( Background Activity Moderator)



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
{4d36e972-e325-11ce-bfc1-08002be10318}	=
{53f56307-b6bf-11d0-94f2-00a0c91efb8b}	
{6bdd1fc6-810f-11d0-bec7-08002be2092f}	
AppCompatCache	
<b>bam</b>	
State	
UserSettings	
S-1-5-18	

Bookmark information

Hive

Category

Name

Key path

Short description

Long description

Total rows: 17 Export ?

Type viewer

Value name: Version

Value type: RegDword

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

13:08 09-07-2023

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	13-09-08	File	11,008 KB
SOFTWARE	13-10-55	Text Document	2,476 KB
SOFTWARE	13-09-08	File	68,608 KB
SECURITY	13-10-55	Text Document	4 KB
SECURITY	13-09-08	File	32 KB
SAM	13-10-55	Text Document	8 KB
SAM	13-09-08	File	64 KB
NTUSER	13-11-02	Text Document	39 KB
NTUSER	13-09-07	DAT File	1,024 KB
DEFAULT	13-10-55	Text Document	16 KB
DEFAULT	13-09-08	File	512 KB

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

System.txt file edit with  
Notepad++.

14 items | 1 item selected 372 KB

13:09 09-07-2023



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 - Microsoft.Windows.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_cw5nlh2txyewy
```

## 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_65a
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.svs,Kernel driver,%
```



## 2. AppCompactcache Analysis/Shimcache

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

File Home Share View Application Tools Manage Get-ZimmermanTools

Pin to Quick access Copy Paste Cut Copy path Move to Copy to Delete Rename New folder New item Open Easy access Properties Select all Select none Invert selection

Clipboard Organize New Open Select

Back Forward Up This PC SDT\_x64FREE\_EN-US\_VHD (C:) Tools Get-ZimmermanTools Search Get-ZimmermanTools

Evidence Execution NTFS Registry This PC 3D Objects Desktop Documents Downloads Music Pictures Videos SDT\_x64FREE\_EN CD Drive (D:) Virtual Downloads (\\\) Network

Name	Date modified	Type	Size
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	
SQLECmd	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
RBCmd	05-08-2022 13:05	Application	3,607 KB

32 items 1 item selected 4.41 MB

Using this location open this file in cmd.

Windows Search File Explorer Task View Internet Explorer File Explorer Mozilla Firefox 16:18 02-08-2023 1

# Go to the Appcompatcacheparser.exe in cmd

The image shows a Windows Server 2019 Datacenter Evaluation desktop environment. A Command Prompt window is open, running as Administrator, with the path C:\Windows\System32\cmd.exe. The window title is "Administrator: C:\Windows\System32\cmd.exe". The desktop background is dark blue, and the taskbar at the bottom includes icons for File Explorer, Edge, and other standard Windows applications.

```
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.

The screenshot shows a Windows Server 2019 Datacenter Evaluation desktop environment. A Command Prompt window titled "Administrator: C:\Windows\System32\cmd.exe" is open, displaying the help documentation for the AppCompatCacheParser.exe tool. The command listed is:

```
--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
```

Below the help text, the command is run:

```
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>

User accounts\_V...

Windows Server 2019 Datacenter Evaluation  
Windows License valid for 173 days  
Build 17763.rs5\_release.180914-1434

06:11 05-07-2023



Recycle Bin

AccessData

FTK Image



Firefox



Event Log  
Explorer



Notepad++



book



User  
accounts\_V...

File Explorer

Execution

File Home Share View

Cases Analysis Execution

Evidence plugins Registry

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- SDT\_x64FREE\_EN

CD Drive (D:) Vir

28 1 item

20230705061123\_Windows10C\_11\_SYSTEM... 05-07-2023 06:11 CSV File

Show the file in Execution folder.

Windows Server 2019 Datacenter Evaluation

Windows License valid for 173 days

Build 17763.rs5\_release.180914-1434



06:12  
05-07-2023

Drag a column header here to group by that column

Enter text to search...

Find

# Output show in Timeline Explorer.

	Line	Tag	Control S...	Duplicate	Cache Entry Posi...	Executed	Last Modified Time UTC	Path
▼	=	■	=	■	=	RBC	=	RBC
▶	1	□		1	□	0 No	2021-10-06 13:52:38	C:\Windows\system32\sp
	2	□		1	□	1 No		00000009 000a564b2739e
	3	□		1	□	2 No		00000009 000b08a200000
	4	□		1	□	3 No		00000009 00010000f0970
	5	□		1	□	4 No		00000009 000c005f0bb90
	6	□		1	□	5 No		00000009 000b08ff00050
	7	□		1	□	6 No	2023-06-29 08:25:43	C:\Program Files\Wind
	8	□		1	□	7 No		00000009 000f00630c820
	9	□		1	□	8 No		00000009 0012090104c60
	10	□		1	□	9 No	2023-06-29 08:13:18	C:\ProgramData\Micros
	11	□		1	□	10 No	2023-06-29 08:24:59	C:\Program Files\Wind
	12	□		1	□	11 Yes		00000009 00015a0c00790
	13	□		1	□	12 No	2023-06-29 08:24:55	C:\Program Files\Wind
	14	□		1	□	13 No		00000009 000b090000000
	15	□		1	□	14 No		00000009 00015a0c00790
	16	□		1	□	15 No		00000009 0004089c33f70
	17	□		1	□	16 Yes		00000009 07e7272e697a0
	18	□		1	□	17 No	2023-06-29 08:22:37	C:\Program Files\Wind
	19	□		1	□	18 No		00000009 000b090000020

```

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 09:08:052
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_cw5n1h2txy
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 cw5n1h2txyewy 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 what:  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++



### **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 desktop environment. On the left, a File Explorer window displays a folder structure under 'This PC'. In the center, a Registry Explorer window is open, showing the contents of the 'Amcache.hve' file.

**File Explorer (Left):**

- Path: This PC > SDT\_x64FREE\_EN-US\_VHD (C:) > Cases > F > Windows > AppCompat > Programs
- Selected item: Amcache.hve (HVE File, 1,280 KB)

**Registry Explorer (Right):**

- Version: Registry Explorer v1.6.0.0
- Menu: File, Tools, Options, Bookmarks (0/0), View, Help
- Tabs: Registry hives (1) [selected], Available bookmarks (0/0)
- Search bar: Enter text to search...
- Table (Key name):

Key name	# values	# subkeys	Last write timestamp
RBC	=	=	=
C:\Cases\F\W...			2023-06-28 17:12:
{11517B7C...}	2	1	2023-06-28 17:12:
Associated de...	0	0	
- Table (Values):

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

**Taskbar (Bottom):**

- Icons: Start, Search, Task View, Edge, File Explorer, Mozilla Firefox, Registry Explorer
- System tray: 16:38, 09-07-2023

## Registry Explorer v1.6.0.0

File Tools Options Bookmarks (0/0) View Help

Registry hives (1)

Available bookmarks (0/0)

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 0b0ceee...	19	
appinstaller.exe c736df...	19	
appinstallerelev a8a669...	19	
appinstallerpyth 67732a...	19	
calculator.exe 724943cb...	19	
codecpacks.heif. 7decc...	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	

Values Amcache-InventoryApplicationFile

Drag a column header here to group by that column

	Timestamp	Path	Name	Product Name	Publisher	Version	SHA1
▼	2023-06-29 0...	c:\program files\windowsapps\microsoft.microsoft3dviewer_6.1908.2042.0_x64_8wekyb3d8bbwe\3dviewer.exe	3DViewer.exe	view 3d	microsoft corporation	6.1908.2042.0	ee05f81b330d2e755d8028ec5da859cf9eae1813
▶	2023-06-29 0...	c:\program files\windowsapps\microsoft.desktopappinstall_desktopappinstall_1.0.30251.0_x64_8wekyb3d8bbwe\appinstaller.exe	AppInstaller.exe	microsoft appx click handler	microsoft corporation	1.0.1901.25001	828d5cf25052ad0686636867130f5a8ff4b71a83
▼	2023-06-29 0...	c:\program files\windowsapps\microsoft.desktopappinstall_desktopappinstall_1.0.30251.0_x64_8wekyb3d8bbwe\appinstalle...	AppInstallerElevatedAppServiceClient.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

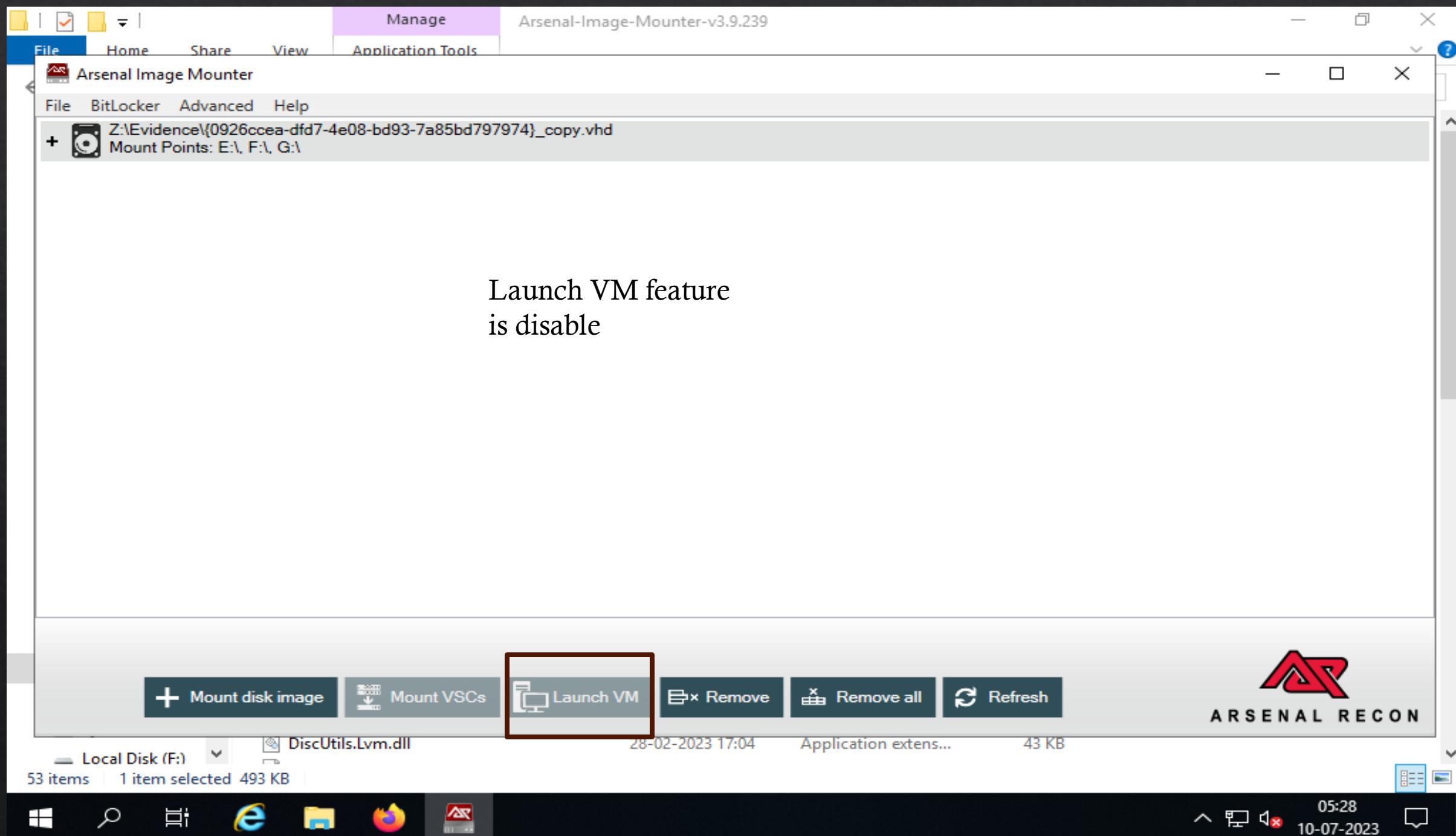
Last write: 2023-06-29 08:12:32

2 of 2 values shown (100.00%)

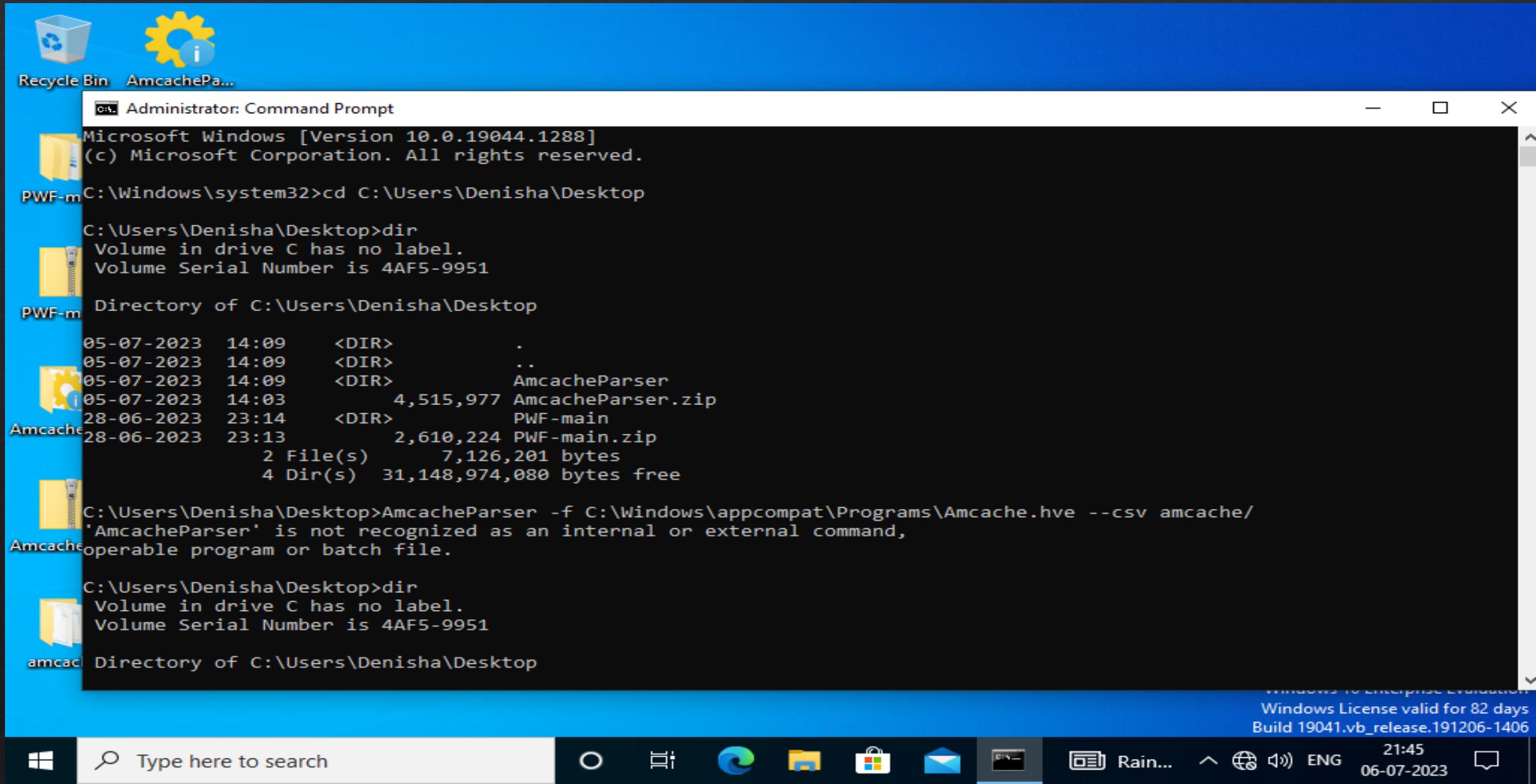
Load complete

Hidden keys: 0 1

17:06  
09-07-2023



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

PWF-m          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

Amcache          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

amcac          Directory of C:\Users\Denisha\Desktop

Windows 10 Enterprise Evaluation
Windows License valid for 82 days
Build 19041.vb_release.191206-1406
21:45
Type here to search  Rain...  ENG  06-07-2023  21:45
```

Recycle Bin AmcachePa...

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/
PWF-m 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/
PWF-m 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...

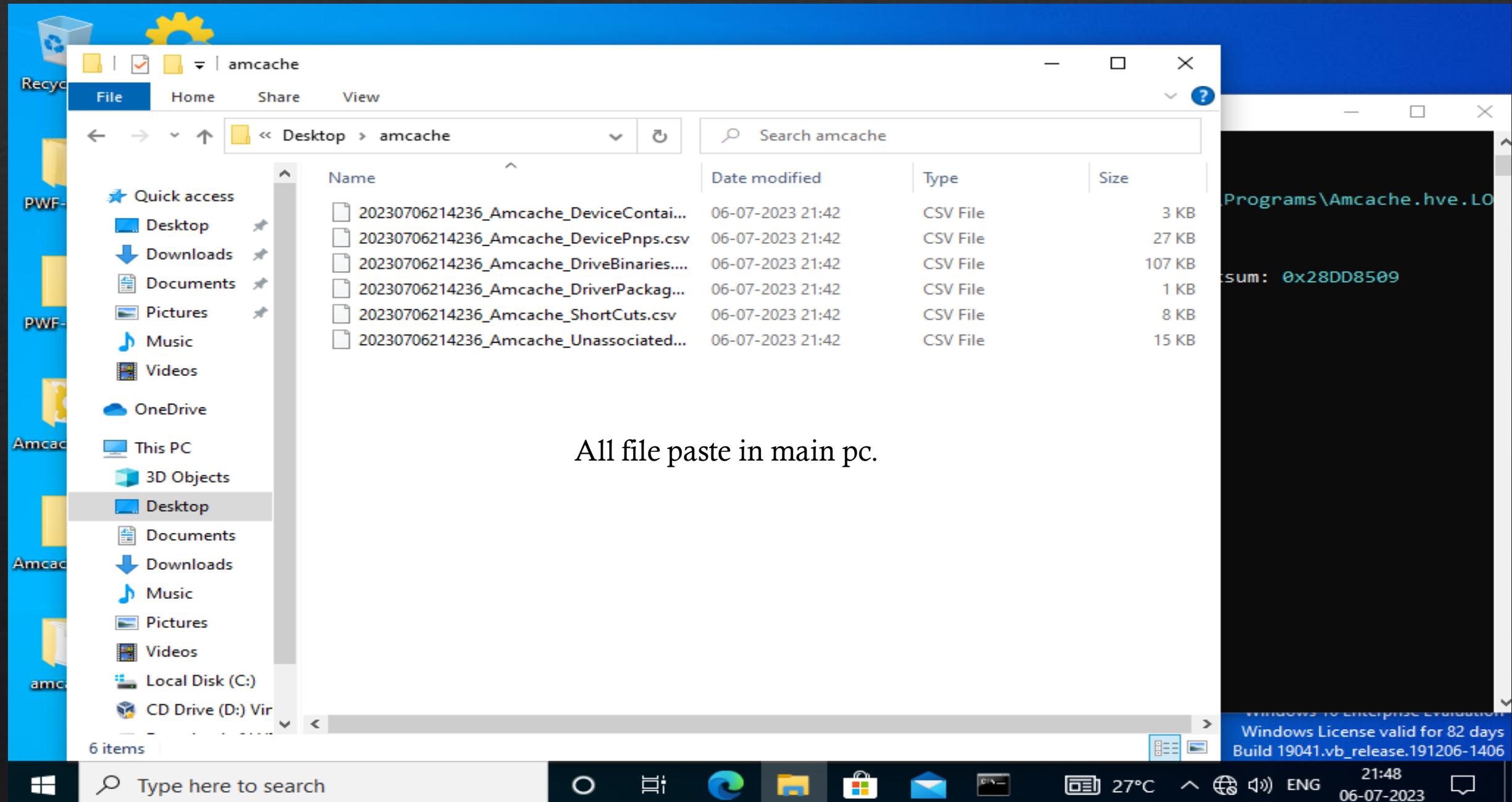
Two transaction logs found. Determining primary log...
Primary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG1, secondary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
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!
amcac Total file entries found: 131
Total shortcuts found: 50
Total device containers found: 9
```

Windows License valid for 82 days  
Build 19041.vb\_release.191206-1406

Type here to search

21:44  
06-07-2023

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



File Home Share View

← → ⌂ ⌃ ⌄ This PC > Downloads > amcache

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

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- 46
- 48
- 49
- Screenshots

OneDrive

This PC

- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- New Volume (C:)
- New Volume (F:)

Network

6 items | 1 item selected 14.0 KB

Type here to search

10:30 10-07-2023

2

20230706214236\_Amcache\_UnassociatedFileEntries - Excel

File Home Insert Draw Page Layout Formulas Data Review View Help Table Design Sign in Tell me what you want to do

Table Name: Table1 Summarize with PivotTable Remove Duplicates Insert Slicer Export Refresh External Table Data Header Row Total Row Banded Rows First Column Last Column Banded Columns Filter Button Quick Styles Table Styles

A5 Unassociated

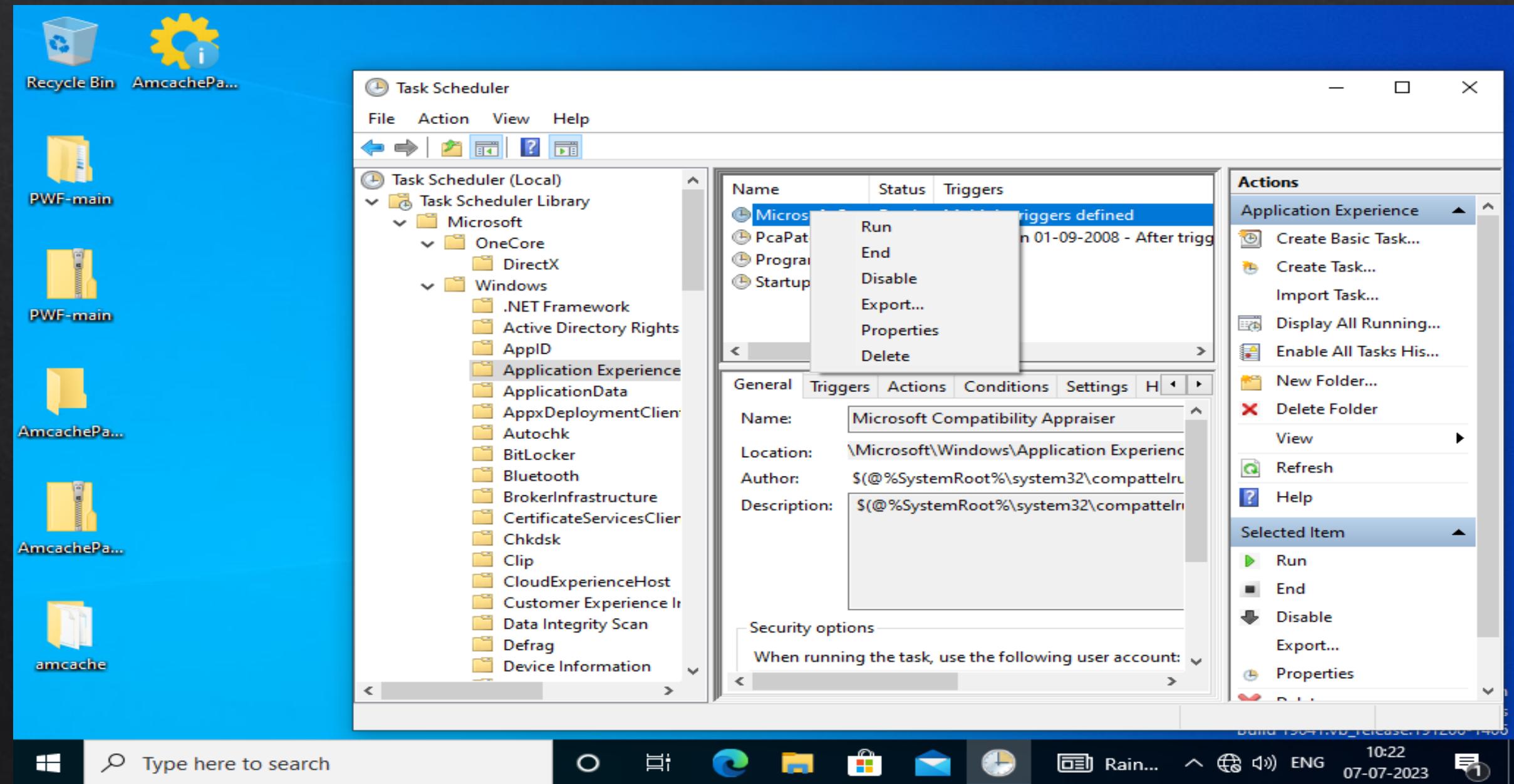
**Amcache Entry**

Column16364	ProgramId	FileKeyLastWriteTimestamp	SHA1	IsOsComponent	FullPath	Name	FileExtension	LinkDate	Prod
Unassociated	0006a8dc383d	05-07-2023 08:39	32136ffefc	FALSE	c:\users\de	AmcacheF.exe	.exe	24-10-2052 08:04	amc
Unassociated	0000f519feec	29-06-2023 08:08	77f2e744c	TRUE	c:\windows\CompatTe	.exe	.exe	18-10-2025 04:45	microsoft
Unassociated	0006f3904a4b	29-06-2023 08:09	074349c30	FALSE	c:\program	cookie_ex.exe	.exe	21-06-2023 22:30	microsoft
Unassociated	0000f519feec	29-06-2023 08:01	11eba7b1	TRUE	c:\windows\csrss.exe	.exe	.exe	25-05-1971 13:07	microsoft
Unassociated	0000f519feec	29-06-2023 08:08	0646f8653	TRUE	c:\windows\DeviceCer	.exe	.exe	19-05-2039 12:13	microsoft
Unassociated	0006f3904a4b	29-06-2023 08:09	777ac620a	FALSE	c:\program	elevation.exe	.exe	21-06-2023 22:30	microsoft
Unassociated	0006f3904a4b	29-06-2023 08:09	872cc644f	FALSE	c:\program	identity_h.exe	.exe	21-06-2023 22:30	microsoft
Unassociated	0006e0870de2	29-06-2023 08:09	5dedd60f	FALSE	c:\program	ie_to_edg.exe	.exe	21-06-2023 22:30	internet explorer
Unassociated	0006ae478658	29-06-2023 08:09	690897252	FALSE	c:\program	MicrosoftI.exe	.exe	06-06-2023 18:16	microsoft
Unassociated	0006868509b0	29-06-2023 08:09	7f6daa619	FALSE	c:\program	MicrosoftI.exe	.exe	06-06-2023 18:15	microsoft
Unassociated	0006868509b0	29-06-2023 08:09	076f72b14	FALSE	c:\program	MicrosoftI.exe	.exe	06-06-2023 18:16	microsoft
Unassociated	0006868509b0	29-06-2023 08:09	9f5c3fd02	FALSE	c:\program	MicrosoftI.exe	.exe	06-06-2023 18:22	microsoft
Unassociated	0006868509b0	29-06-2023 08:09	9f5c3fd02	FALSE	c:\program	MicrosoftI.exe	.exe	06-06-2023 18:22	microsoft
Unassociated	00060cab34c3	28-06-2023 17:12	3d26b0dc5	FALSE	c:\program	MicrosoftI.exe	.exe	22-07-2021 01:16	microsoft
Unassociated	0006868509b0	29-06-2023 08:09	b61a5756c	FALSE	c:\program	MicrosoftI.exe	.exe	06-06-2023 18:16	microsoft
Unassociated	0006868509b0	29-06-2023 08:09	7f7c48ad1	FALSE	c:\program	MicrosoftI.exe	.exe	06-06-2023 18:16	microsoft
Unassociated	0006868509b0	29-06-2023 08:09	cc92d47f7	FALSE	c:\program	MicrosoftI.exe	.exe	06-06-2023 18:15	microsoft
Unassociated	000651e5db32	29-06-2023 08:09	7c51ea622	FALSE	c:\program	MicrosoftI.exe	.exe	21-06-2023 22:30	microsoft
Unassociated	000651e5db32	29-06-2023 08:09	7c51ea622	FALSE	c:\program	MicrosoftI.exe	.exe	21-06-2023 22:30	microsoft
Unassociated	0000f519feec	29-06-2023 08:04	7e29a8d98	TRUE	c:\windows\MoUsCoI	.exe	.exe	01-05-2068 18:03	microsoft
Unassociated	0006f3904a4b	29-06-2023 08:09	fea1f23ec	FALSE	c:\program	msedge.e.exe	.exe	21-06-2023 22:30	microsoft
Unassociated	0006707b1ec4	29-06-2023 08:09	92332ecf2	FALSE	c:\program	msedgew.exe	.exe	21-06-2023 22:30	microsoft

20230706214236\_Amcache\_Unassoci

Ready Accessibility: Unavailable Display Settings 10:29 10-07-2023

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



10:37  
10-07-2023



amcache2				
File	Home	Share	View	?
< > ▲ ▼ This PC > Downloads > amcache2				
Quick access	Name	Date modified	Type	Size
Desktop	20230710103733_Amcache_DeviceContai...	10-07-2023 10:37	Microsoft Excel C...	3 KB
Downloads	20230710103733_Amcache_DevicePnps	10-07-2023 10:37	Microsoft Excel C...	32 KB
Documents	20230710103733_Amcache_DriveBinaries	10-07-2023 10:37	Microsoft Excel C...	108 KB
Pictures	20230710103733_Amcache_DriverPackages	10-07-2023 10:37	Microsoft Excel C...	1 KB
46	20230710103733_Amcache_ShortCuts	10-07-2023 10:37	Microsoft Excel C...	8 KB
48	20230710103733_Amcache_Unassociated...	10-07-2023 10:37	Microsoft Excel C...	18 KB
49				
Screenshots				
OneDrive				
This PC				
Desktop				
Documents				
Downloads				
Music				
Pictures				
Videos				
New Volume (C:)				
New Volume (F:)				
Network				

Save the file Amcache2 folder and open with excel.

6 items



Type here to search



10:40  
10-07-2023



Table Name:	Summarize with PivotTable	Insert Slicer	<input checked="" type="checkbox"/> Header Row	<input type="checkbox"/> First Column	<input checked="" type="checkbox"/> Filter Button
Table1	Remove Duplicates	Export Refresh	<input type="checkbox"/> Total Row	<input type="checkbox"/> Last Column	
Resize Table	Convert to Range	External Table Data	<input checked="" type="checkbox"/> Banded Rows	<input type="checkbox"/> Banded Columns	
Properties	Tools				
					Table Style Options
					Table Styles

Output  
Updated.

	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	0006119b97889343334d	10-07-2023 04:53	42d834da	FALSE	c:\program cookie_ex.exe	# #####	# #####	
5	Unassociated	0000f519feec486de87e	29-06-2023 08:01	11eba7b1	TRUE	c:\windows csrss.exe	.exe	# #####	
6	Unassociated	0000f519feec486de87e	29-06-2023 08:08	0646f8653	TRUE	c:\windows DeviceCer.exe	# #####	# #####	
7	Unassociated	0006119b97889343334d	10-07-2023 04:53	3bd5d28ca	FALSE	c:\program elevation.exe	# #####	# #####	
8	Unassociated	0006119b97889343334d	10-07-2023 04:53	cdf846712	FALSE	c:\program identity_h.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	0006aa1f8992cfa6e338t	10-07-2023 04:53	06bac910a	FALSE	c:\program Microsoftl.exe	# #####	# #####	
12	Unassociated	0006aa1f8992cfa6e338t	08-07-2023 15:53	aa15234f0	FALSE	c:\program Microsoftl.exe	# #####	# #####	
13	Unassociated	0006aa1f8992cfa6e338t	08-07-2023 15:53	fed2634cd	FALSE	c:\program Microsoftl.exe	# #####	# #####	
14	Unassociated	0006aa1f8992cfa6e338t	08-07-2023 15:53	ed6642a2c	FALSE	c:\program Microsoftl.exe	# #####	# #####	
15	Unassociated	0006aa1f8992cfa6e338t	08-07-2023 15:53	0c5f3e8a7	FALSE	c:\program Microsoftl.exe	# #####	# #####	
16	Unassociated	00060cab34c3bd2ce1cf	28-06-2023 17:12	3d26b0dcf	FALSE	c:\program Microsoftl.exe	# #####	# #####	
17	Unassociated	0006aa1f8992cfa6e338t	08-07-2023 15:53	06bac910a	FALSE	c:\program Microsoftl.exe	# #####	# #####	
18	Unassociated	0006aa1f8992cfa6e338t	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	7e29a8d98	TRUE	c:\windows MoUsCoI.exe	# #####	# #####	
22	Unassociated	0006e71e182965d4146f	10-07-2023 04:53	f92f04998	FALSE	c:\program MpCopyA.exe	# #####	# #####	
23	Unassociated	0006dc1a176320b5dbbe	10-07-2023 04:53	45d7b8e91	FALSE	c:\windows MoSigStul.exe	# #####	# #####	

20230710103733\_Amcache\_Unassoci

Ready

Accessibility: Unavailable

Display Settings



10:50  
10-07-2023

## 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.

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

- Title Bar:** prefetch
- Toolbar:** File, Customize Quick Access Toolbar, Back, Forward, Up, Refresh, Search prefetch, Help.
- Address Bar:** C:\Cases\F\Windows\prefetch
- Left Sidebar:** Quick access, 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 (\\\W).
- Table Headers:** Name, Date modified, Type, Size
- Table Data:** A list of 180 items, each a PF File, mostly named after system processes like AM\_BASE.EXE, BACKGROUNDTASKHOST.EXE, and DLLHOST.EXE, with sizes ranging from 2 KB to 25 KB.
- Bottom Status:** 180 items, 06:07, 07-07-2023.

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
BYTCODEGENERATOR.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
CVTRRES.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

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

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

- Title Bar:** Manage, Get-ZimmermanTools
- Toolbar:** File, Home, Share, View, Application Tools
- Address Bar:** C:\Tools\Get-ZimmermanTools
- Search Bar:** Search Get-ZimmermanTools
- Left Pane (Navigation):** 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:), Downloads (\\\)\
- Right Pane (List View):**

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	
SQLECmd	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
<b>PECmd</b>	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-3FBEF7FD.pf"  
PECmd.exe -f "C:\Temp\CALC.EXE-3FBEF7FD.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 <a href="https://goo.gl/CNVq0k">https://goo.gl/CNVq0k</a> for options [default: yyyy-MM-dd HH:mm:ss]



06:08  
07-07-2023

```
c:\ 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: 1
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.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.SC  
ALE-100\_8WEKYB3D8BBWE  
03: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB\_18.1903.1152.0\_NEUTRAL\_SPLIT.SC  
ALE-100\_8WEKYB3D8BBWE\IMAGES  
04: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB\_18.1903.1152.0\_X64\_\_8WEKYB3D8BB  
WE  
05: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB\_18.1903.1152.0\_X64\_\_8WEKYB3D8BB  
WE\MICROSOFT.SYSTEM.PACKAGE.METADATA  
06: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSSTORE\_11910.1002.5.0\_NEUTRAL\_SPLIT.SCALE-10  
0\_8WEKYB3D8BBWE  
07: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSSTORE\_11910.1002.5.0\_NEUTRAL\_SPLIT.SCALE-10  
0\_8WEKYB3D8BBWE\ASSETS  
08: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSSTORE\_11910.1002.5.0\_NEUTRAL\_SPLIT.SCALE-10  
0\_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\IMMERSIVECONTROLPANEL  
14: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\IMMERSIVECONTROLPANEL\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



## 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\INETCACHE\MSIMGSIZ.DAT
205: \VOLUME{\01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\WINDOWSCODECS.DLL
206: \VOLUME{\01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_X64_8WEKYB3D8BBWE\MYOFFICE.RUNTIMECOMPONENTS.WINMD
207: \VOLUME{\01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_X64_8WEKYB3D8BBWE\MYOFFICE.RUNTIMECOMPONENTS.DLL
208: \VOLUME{\01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.VCLIBS.140.00_14.0.27323.0_X64_8WEKYB3D8BBWE\MSVC140_APP.DLL
209: \VOLUME{\01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.VCLIBS.140.00_14.0.27323.0_X64_8WEKYB3D8BBWE\VCRUNTIME140_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\INETCACHE\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\INETCACHE\S3F01B3R\THIRDPARTYNOTICE[1].HTM
215: \VOLUME{\01d9aa46f526b4aa-4af59951}\WINDOWS\SYSTEM32\CRYPTOWINRT.DLL
216: \VOLUME{\01d9aa46f526b4aa-4af59951}\USERS\DENISHA\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTOFFICEHUB_8WEKYB3D8BBWE\LOCALSTATE\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_SYSTEM...	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

Open this file in timeline explorer



11 items | 1 item selected 1.34 MB

05:24 16-07-2023

# 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

Enter text to search... Find

Note	Source	Filename	Volume	Serial	Source	Created	Source	Modified	Source	Age
▼	File	C:\Cases\F\Windows\prefetch\AM_BASE.EXE-808FC88...	Volume1	SerialC	=	2023-06-29 08:06:55	=	2023-06-29 0...	2023-06-29 0...	2023-06-29 0...
		C:\Cases\F\Windows\prefetch\AM_DELTA.EXE-B7261F...				2023-06-29 08:07:23		2023-06-29 0...	2023-06-29 0...	2023-06-29 0...
		C:\Cases\F\Windows\prefetch\AM_ENGINE.EXE-69ACF...				2023-06-29 08:06:22		2023-06-29 0...	2023-06-29 0...	2023-06-29 0...
		C:\Cases\F\Windows\prefetch\APPLICATIONFRAMEHOS...				2023-06-28 16:24:19		2023-06-29 0...	2023-06-29 0...	2023-06-29 0...
		C:\Cases\F\Windows\prefetch\AUDIODG.EXE-BDFD302...				2023-06-28 16:14:35		2023-06-29 0...	2023-06-29 0...	2023-06-29 0...
		C:\Cases\F\Windows\prefetch\BACKGROUNDTASKHOST ...				2023-06-28 16:20:20		2023-06-28 1...	2023-06-28 1...	2023-06-28 1...
		C:\Cases\F\Windows\prefetch\BACKGROUNDTASKHOST ...				2023-06-28 16:21:51		2023-06-29 0...	2023-06-29 0...	2023-06-29 0...
		C:\Cases\F\Windows\prefetch\BACKGROUNDTRANSFERH...				2023-06-28 16:46:00		2023-06-28 1...	2023-06-28 1...	2023-06-28 1...
		C:\Cases\F\Windows\prefetch\BACKGROUNDTRANSFERH...				2023-06-28 16:24:21		2023-06-28 1...	2023-06-28 1...	2023-06-28 1...
		C:\Cases\F\Windows\prefetch\BACKGROUNDTRANSFERH...				2023-06-28 16:52:04		2023-06-28 1...	2023-06-28 1...	2023-06-28 1...
		C:\Cases\F\Windows\prefetch\BYTECODEGENERATOR.E...				2023-06-28 16:10:07		2023-06-29 0...	2023-06-29 0...	2023-06-29 0...
		C:\Cases\F\Windows\prefetch\CLOUDEXPERIENCEHOST...				2023-06-28 16:14:15		2023-06-28 1...	2023-06-28 1...	2023-06-28 1...
		C:\Cases\F\Windows\prefetch\CMD.EXE-4A81B364.pf				2023-06-28 16:32:49		2023-06-28 1...	2023-06-28 1...	2023-06-28 1...
		C:\Cases\F\Windows\prefetch\COMPATTELRUNNER.EXE...				2023-06-28 17:13:24		2023-06-28 1...	2023-06-28 1...	2023-06-28 1...
		C:\Cases\F\Windows\prefetch\CONHOST.EXE-1F3E9D7...				2023-06-28 16:13:22		2023-06-29 0...	2023-06-29 0...	2023-06-29 0...
		C:\Cases\F\Windows\prefetch\CONSENT.EXE-531BD9E...				2023-06-28 16:20:43		2023-06-29 0...	2023-06-29 0...	2023-06-29 0...
		C:\Cases\F\Windows\prefetch\CSC.EXE-67679278.pf				2023-06-28 16:42:40		2023-06-28 1...	2023-06-28 1...	2023-06-28 1...
		C:\Cases\F\Windows\prefetch\CSRSS.EXE-3FE41F7E...				2023-06-28 16:20:38		2023-06-28 1...	2023-06-28 1...	2023-06-28 1...
		C:\Cases\F\Windows\prefetch\CVTRES.EXE-F2B7602E...				2023-06-28 16:42:40		2023-06-28 1...	2023-06-28 1...	2023-06-28 1...

## 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

Key name

RE:

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
▼	RBC	RegDWord	0x00000000	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
▶	SecurityHealth	RegExpandSz	%windir%\system32\secu...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
	VBoxTray	RegExpandSz	%SystemRoot%\AppData\Ro...	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

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



05:49

16-07-2023



# Registry Explorer v1.6.0.0

File Tools Options Bookmarks (29/0) View Help

Registry hives (2)

Available bookmarks (59/0)

run|

Key name  RBC

- ▶ 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
RBC	RBC	RBC	RBC	<input type="checkbox"/>	<input 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"/>

Type viewer  Slack viewer  Binary viewer

Value name

Value type

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



05:49  
16-07-2023

Registry

File Home Share View

This PC > SDT\_x64FREE\_EN-US\_VHD (C:) > Cases > Analysis > Registry

Search Registry

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)

14 items | 1 item selected 38.6 KB

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	0:55	Text Document	8 KB
SAM	9:08	File	64 KB
NTUSER.DA	1:02	Text Document	39 KB
NTUSER.DA	9:07	DAT File	1,024 KB
DEFAULT	0:55	Text Document	16 KB
DEFAULT	9:08	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++.

05:49 16-07-2023

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

```
776 2 = Resources
777 0 = The Internet
778 -----
779 run v.20200511
780 (Software, NTUSER.
781 Software\Microsoft
782 LastWrite Time 202
783 MicrosoftEdgeAut
784 OneDrive - "C:\U
785 Software\Microsoft
786 Software\Wow6432No
787 Software\Microsoft
788 Software\Microsoft
789 Software\Microsoft
790 Software\Microsoft
791 Software\Microsoft
792 Software\Microsoft
793 LastWrite Time 202
794 Software\Microsoft
795 Software\Microsoft
796 Software\Microsoft
797 Software\Microsoft
798 Software\Microsoft
799 Software\Microsoft
800 Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not
801 Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce
802 Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.
```

Find

Find Replace Find in Files Find in Projects Mark

Find what: run

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

Transparency  
 On losing focus  
 Always

Find Next Count Find All in Current Document Find All in All Opened Documents Close

Normal text file length : 39,529 lines : 1,000 Ln : 780 Col : 15 Sel : 8 | 1 Windows (CR LF) ANSI INS

05:51 16-07-2023

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

```
776 2 = Resources
777 0 = The Internet
778 -----
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.exe"
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



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.

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.

```
① Select forensic@WIN-AJDB7GOIQUEJ: /mnt/c/Cases/Analysis/NTFS
forensic@WIN-AJDB7GOIQUEJ:/mnt/c/Cases$ cd ../../..
forensic@WIN-AJDB7GOIQUEJ:/$ cd /mnt/c/Cases/Analysis/NTFS
forensic@WIN-AJDB7GOIQUEJ:/mnt/c/Cases/Analysis/NTFS$ ls -l
total 58904
-rwxrwxrwx 1 forensic forensic 60316000 Jul 1 16:42 MFT.csv
forensic@WIN-AJDB7GOIQUEJ:/mnt/c/Cases/Analysis/NTFS$ grep startup MFT.csv
14800,1,True,5280,1,..\Windows\WinSxS,amd64_microsoft-windows-s..32_kf_commonstartup_31bf3856ad364e35_10.0.19041.1_none_b2014b
56ea660ec9,,0,1,,True,False,True,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,,$DSC,
14985,1,True,5280,1,..\Windows\WinSxS,amd64_microsoft-windows-s..estartup-change-pin_31bf3856ad364e35_10.0.19041.1237_none_66
f7346099d6350,,0,1,,True,False,True,False,None,Windows,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,2023-06-29 05:32:50.0439843,2023-06-29 05:03:11.2621355,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,0,185379446,551,,$DSC,
14986,1,True,14985,1,..\Windows\WinSxS\amd64_microsoft-windows-s..estartup-change-pin_31bf3856ad364e35_10.0.19041.1237_none_66
5f7346099d6350,f,,0,1,,True,False,True,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,,$DSC,
14987,1,True,14985,1,..\Windows\WinSxS\amd64_microsoft-windows-s..estartup-change-pin_31bf3856ad364e35_10.0.19041.1237_none_66
5f7346099d6350,r,,0,1,,True,False,True,False,None,DosWindows,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,2023-06-29 05:32:50.0439843,2023-06-29 05:03:11.2621355,2021-10-06 13:54:23.7551351,2023-06-29 05:03:11.2621355,0,185379310,551,,$DSC,
15238,1,True,5280,1,..\Windows\WinSxS,amd64_microsoft-windows-s..ngshandlers-startup_31bf3856ad364e35_10.0.19041.746_none_522
01f930d0ca36,,0,1,,True,False,True,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,,$DSC,
15239,1,True,15238,1,..\Windows\WinSxS\amd64_microsoft-windows-s..ngshandlers-startup_31bf3856ad364e35_10.0.19041.746_none_522
701f930d0ca36,f,,0,1,,True,False,True,False,None,DosWindows,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,2023-06-29 05:32:50.1371573,2023-06-29 05:03:11.4972405,2021-10-06 13:52:12.3431456,2023-06-29 05:03:11.4972405,0,185417687,551,,$DSC,
15240,1,True,15238,1,..\Windows\WinSxS\amd64_microsoft-windows-s..ngshandlers-startup_31bf3856ad364e35_10.0.19041.746_none_522
701f930d0ca36,r,,0,1,,True,False,True,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_ec3fd4
10728598b3,,0,1,,True,False,True,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 09:51:55
```



```
>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,,174624611,587,,$DSC,  
95546,1,True,24202,1,.\Windows\WinSxS\wow64_microsoft-windows-securestartup-core_31bf3856ad364e35_10.0.19041.1237_none_b3f20c  
1adb3de92\r,fveapibase.dll,.dll,9395,1,,False,False,False,True,False,Archive,Windows,2021-10-06 13:54:19.8017226,2023-  
06-29 05:31:49.2620434,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.2620434,2023-06-29 05:31:49.2620434,,2021-10-06 13:54:  
19.8017226,2023-06-29 05:31:49.2620434,,174624639,587,,$DSC,  
95547,1,True,24201,1,.\Windows\WinSxS\wow64_microsoft-windows-securestartup-core_31bf3856ad364e35_10.0.19041.1237_none_b3f20c  
1adb3de92\f,fveapibase.dll,.dll,16379,1,,False,False,False,True,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,,174624723,587,,$DSC,  
95550,1,True,24202,1,.\Windows\WinSxS\wow64_microsoft-windows-securestartup-core_31bf3856ad364e35_10.0.19041.1237_none_b3f20c  
1adb3de92\r,fveapi.dll,.dll,28304,1,,False,False,False,True,False,Archive,DosWindows,2021-10-06 13:54:19.8017226,2023-  
06-29 05:31:49.3104659,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.3104659,2023-06-29 05:31:49.3104659,,2021-10-06 13:54:  
19.8017226,2023-06-29 05:31:49.3104659,,174624787,587,,$DSC,  
105628,9,True,105627,9,.\AtomicRedTeam\atomics\T1547.001\src,batstartup.bat,.bat,34,1,,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,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,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



06:16  
16-07-2023

# 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 shows the Windows Task Manager window with the 'Services' tab selected. The window displays a list of services with columns for Name, PID, Description, Status, and Group. The 'Status' column indicates whether each service is Running or Stopped. The 'Group' column shows the service's classification. A legend at the bottom left identifies icons for 'Fewer details' and 'Open Services'. The bottom right corner of the screen shows the Windows Server 2019 Datacenter Evaluation status, including the license period and build number. The taskbar at the bottom includes icons for File Explorer, Edge, File Explorer, and Task View.

Name	PID	Description	Status	Group
AJRouter		AllJoyn Router Service	Stopped	LocalServiceN...
ALG		Application Layer Gateway Service	Stopped	LocalServiceN...
AppIDSvc		Application Identity	Stopped	netsvcs
Appinfo		Application Information	Stopped	netsvcs
AppMgmt		Application Management	Stopped	AppReadiness
AppReadiness		App Readiness	Stopped	
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

Fewer details | Open Services

Windows Server 2019 Datacenter Evaluation  
Windows License valid for 161 days  
Build 17763.rs5\_release.180914-1434

08:12 16-07-2023

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (29/0) View Help

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

Key name

RBC

- 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	Description	Display Name	Start Type	Service Status	Name	Parameter	Group	Image File	Service State	Required Privileges
3ware			Boot	Kernel	2023-07-16 07:54:00	2019-12-10 10:00:00	SCSI miniport	System32\drivers\3ware.sys	Running	SeImpersonatePrivilege
AarSvc	@%SystemRoot%\system32\AarSvc.dll,-101	@%SystemRoot%\system32\AarSvc.dll,-100	Manual	96	2019-12-10 10:00:00	2019-12-10 10:00:00	%SystemRoot%\system32\svchost.exe-k AarSvcGroup -p	%SystemRoot%\System32\AarSvc.dll	Stopped	SeImpersonatePrivilege
ACPI		@acpi.inf,%ACPI.SvcDescriptor%;Microsoft ACPI Driver	Boot	Kernel	2023-07-16 07:54:00	2023-07-16 07:54:00	Core	System32\drivers\ACPI.sys	Running	
AcpiDev		@acpidev.inf,%AcpiDev.	Manual	Kernel	2019-12-10 10:00:00	2019-12-10 10:00:00	Extended Base	\SystemRoot\System32\	Stopped	

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

```
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.

# Detecting and Analyzing scheduled tasks

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (29/0) View Help

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

Enter text to search... Find

Key name

System  
TaskCache  
  Boot  
  Logon  
  Maintenance  
Plain  
Tasks {0016B09F-CFDA-4F5B-A70B-84A75599B89B}

Bookmark information

Hive

Category

Name

Key path

Short description

Long description

Load the Software hive on Registry Editor and click taskcache then click task

Values TaskCache

Drag a column header here to group by that column

Version	Key Na...	Path	Create...	Last St...	Last Stop	Task St...	Last Ac...	Source	Descrip...	Author
3	{0016B09F-CFDA-4F5B-A70B-84A75599B89B}	\Microsoft\Windows\DeviceClient\HandleWnsCommand	2023-0...				0	0		
3	{00446CF1-8668-472D-BE DD-D0BB88DBA009}	\Microsoft\Windows\Registry\RegIdl eBackup	2023-0...				0	0	\$(@%systemroot%\system32\regidle.dll,-601)	\$(@%systemroot%\system32\regidle.dll,-602)
3	{008539BF-83F9-4483-9E0A-EEEE6EAC0A08}	\Microsoft\Windows\Shell\UpdateUserPictureTask	2023-0...				0	0		
3	{02579FB1-5050-}	\Microsoft\Window	2023-0...				0	0		

Total rows: 194 Export ?

Type viewer

Key: Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks Value: None Collapse all hives

Selected hive: SYSTEM Last write: 29-06-2023 08:25:03 +00:00 Key contains no values Hidden keys: 0 1

08:44 16-07-2023

Administrator: Command Prompt

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

```
40484
40485    9 - LastWrite time: 2023-06-28 16:32:41Z
40486    Path: file:///C:/[afl17ba98-35d5-43f9-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}
```

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

Windows Notepad Internet Explorer Firefox File Explorer Paint Task View Task Switcher 08:53 16-07-2023 1

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

# Analysis with Sysinternals Autorun tool

## Autoruns for Windows - Sysinternals | Microsoft Learn

what is mean windows services - x | english to gujarati translate - Go x Autoruns for Windows - Sysinternals x +

learn.microsoft.com/en-us/sysinternals/downloads/autoruns

Filter by title

Home

Downloads

Downloads

> File and Disk Utilities

> Networking Utilities

Process Utilities

Process Utilities

AutoRuns

Handle

ListDLLs

Portmon

ProcDump

Process Explorer

Process Monitor

PsExec

PsGetSid

PsKill

PsList

Usage

Autorunsc Usage

Related Links

Download

By Mark Russinovich

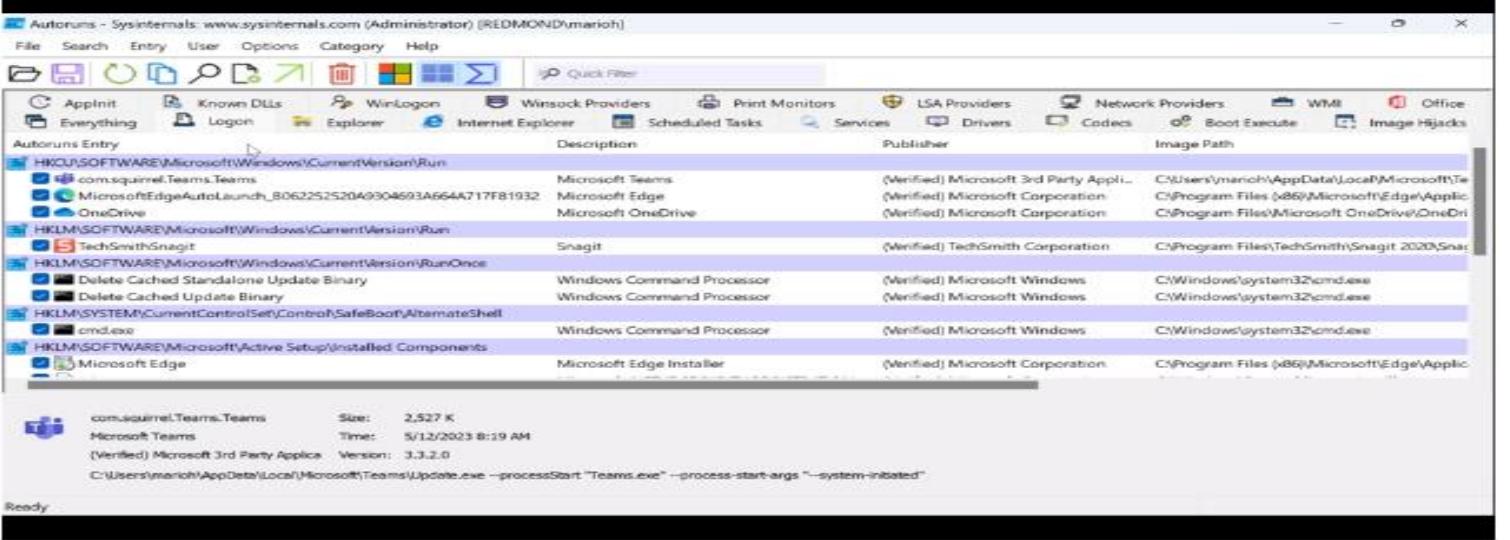
Published: June 27, 2023

 Download Autoruns and Autorunsc (2.8 MB)

Run now from Sysinternals Live.

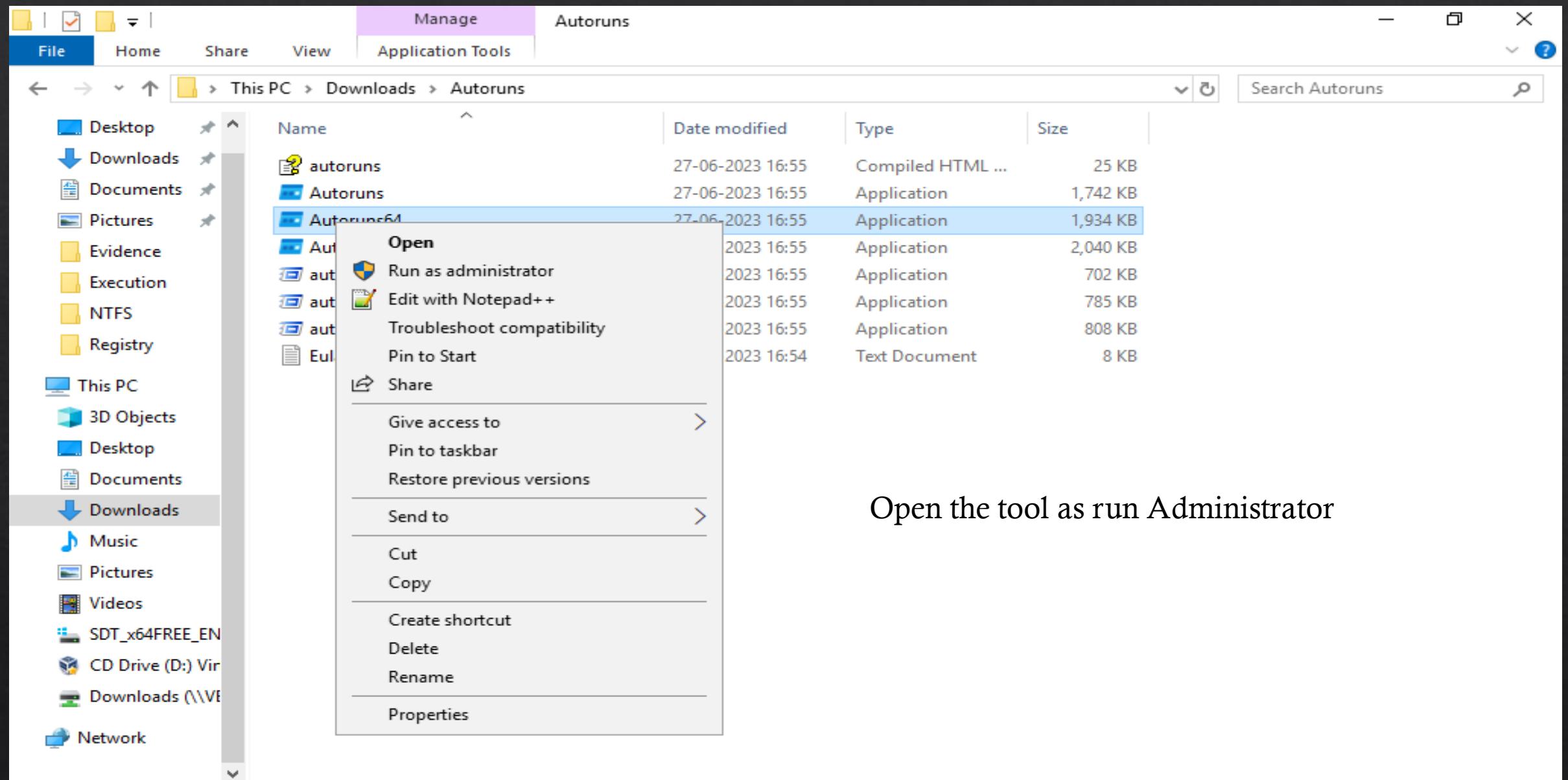
Autorun tools use for detect and Analyze the autorun file like malware and virus Affected file , run file with boot time etc.

Download the tool from microsoft



Type here to search

14:44 16-07-2023



Open the tool as run Administrator

8 items | 1 item selected 1.88 MB |



09:16  
16-07-2023

**File** Search Entry User Options Category Help Open... Ctrl+O  
 Save... Ctrl+S

Quick Filter

Analyze Offline System...

Compare...

Refresh F5

Cancel ESC

Exit

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

Ready



## Offline System

Select the directories of the offline system:

System Root: F:\Windows



User Profile: F:\Users\Denisha



OK

Cancel

		Publisher		Image Path
<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\Loc...
	HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms			
<input checked="" type="checkbox"/>	rdclip	RDP Clipboard Monitor	(Not Verified) Microsoft Corporati...	C:\Windows\system32\rdclip...
	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 Application	(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  
 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

Ready

09:22  
16-07-2023

Autoruns - Sysinternals: www.sysinternals.com (Administrator) [WIN-AJDB7GOIQEJ\Administrator]

File Search Entry User Options Category Help

Quick Filter

Codecs Boot Execute Image Hijacks Applnit Known DLLs Winlogon Winsock Providers Print Monitors  
LSA Providers Network Providers WMI Office  
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers

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\rdpclip
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 Application	(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 Size: 2,311 K Time: 28-06-2023 16:25  
(Verified) Microsoft Corporation Version: 21.220.1024.0005  
"C:\Users\Denisha\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background

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

Ready

09:23 16-07-2023

# 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.

Screenshot of a web browser showing the Windows Security Log Event ID 4624 page from ultimatewindowssecurity.com.

The browser tabs are: what is mean windows, english to gujarati trans, event log analysis in dic, Windows Security Log (active), and others.

The page title is "Windows Security Log Event ID 4624".

The main content area includes:

- Encyclopedia** (highlighted)
- 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.
- Description**: 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**
- Description Fields in 4624**

Right side panel (Operating Systems table):

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

Bottom banner: Enter the event ID and show the detail.

Cookies message: Cookies help us deliver the best experience on our website. By using our website, you agree to the use of cookies. **Accept**

# Analyzing Windows event logs with EventLogExplorer and EvtxCmd

Show The All Event Log Of Target system.

Name	Date modified	Type	Size
Application	29-06-2023 09:07	Event Log	1,092 KB
Microsoft-Client-Licensing-Platform%4A...	29-06-2023 09:07	Event Log	1,028 KB
Microsoft-Windows-AAD%4Operational	28-06-2023 16:31	Event Log	68 KB
Microsoft-Windows-Application-Experi...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-AppModel-Runtime...	29-06-2023 09:07	Event Log	1,028 KB
Microsoft-Windows-AppReadiness%4Ad...	28-06-2023 18:13	Event Log	1,092 KB
Microsoft-Windows-AppReadiness%4Op...	28-06-2023 18:13	Event Log	68 KB
Microsoft-Windows-AppXDeployment%...	29-06-2023 09:07	Event Log	1,028 KB
Microsoft-Windows-AppXDeploymentSe...	29-06-2023 09:07	Event Log	5,124 KB
Microsoft-Windows-AppxPackaging%4O...	29-06-2023 09:07	Event Log	1,028 KB
Microsoft-Windows-Audio%4CaptureM...	28-06-2023 16:05	Event Log	68 KB
Microsoft-Windows-Audio%4Operational	28-06-2023 16:05	Event Log	68 KB
Microsoft-Windows-Authentication User...	28-06-2023 16:31	Event Log	68 KB
Microsoft-Windows-BackgroundTaskInfr...	28-06-2023 18:13	Event Log	68 KB
Microsoft-Windows-Biometrics%4Opera...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-BitLocker%4BitLock...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-Bits-Client%4Operat...	29-06-2023 09:07	Event Log	1,028 KB
Microsoft-Windows-CloudStore%4Opera...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-CodeIntegrity%4Op...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-Containers-BindFlt...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-Containers-Wcifs%4...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-CoreSystem-SmsRo...	29-06-2023 09:07	Event Log	68 KB
Microsoft-Windows-Crypto-DPAPI%4Op...	29-06-2023 09:07	Event Log	68 KB

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

< Load filter >

Objects tree

Search

Application.evtb

Date Time Event Source Category User Computer

	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

11:18 16-07-2023

Open the Event log explorer and load the first event.

Get-ZimmermanTools

File Home Share View

C:\Tools\Get-ZimmermanTools

Search Get-ZimmermanTools

Pictures Evidence Execution NTFS Registry This PC 3D Objects Desktop Documents Downloads Music Pictures Videos SDT\_x64FREE\_EN CD Drive (D:) Virtual System Reserved Local Disk (F:) Local Disk (G:) Downloads (\\\) Network

Name Date modified Type Size

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	
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.

11:20 16-07-2023

Untitled EFLX - Event Log Explorer

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

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

Object: C:\Tools\Get-ZimmermanTools\EvtxECmd>EvtxECmd.exe

Description:

Version: EvtxECmd version 1.5.0.0

>

> Author: Eric Zimmerman (saericzimmerman@gmail.com)

> https://github.com/EricZimmerman/evtx

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 evtx 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.fffffffff]
- inc <inc> List of Event IDs to process. All others are ignored. Overrides --exc Format is 4624,4625,5410  
or try to change Description Server.

The following information was included with the event:  
Windows Defender

Description Data

Windows Internet Explorer File Manager Mozilla Firefox File Explorer Task View Start 11:27 16-07-2023

Untitled EIX - Event Log Explorer

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

```
--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

-f or -d is required. Exiting
```

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

```
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
or try to change Description Server.

The following information was included with the event:
Windows Defender
```

Description Data

Build 17705.1522\_release.100514-1454

11:27 16-07-2023

Eventlogs

File Home Share View

C:\Cases\Analysis\Eventlogs

Search Eventlogs

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

Name Date modified Type Size

20230716112553\_EvtxEcmd\_Output 16-07-2023 11:26 CSV File 28,480 KB

Show the all event output in this file

11:28 16-07-2023

## Show the output

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
T	=	[ ]	=	=	=	=	A B C	A B C
	175	[ ]	175	175	2023-06-28 16...	15	Info	SecurityCenter
	176	[ ]	176	176	2023-06-28 16...	16394	Info	Microsoft-Windows-Security-
	177	[ ]	177	177	2023-06-28 16...	15	Info	SecurityCenter
	178	[ ]	178	178	2023-06-28 16...	15	Info	SecurityCenter
	179	[ ]	179	179	2023-06-28 16...	15	Info	SecurityCenter
	180	[ ]	180	180	2023-06-28 16...	16384	Info	Microsoft-Windows-Security-
	181	[ ]	181	181	2023-06-28 16...	16394	Info	Microsoft-Windows-Security-
	182	[ ]	182	182	2023-06-28 16...	16384	Info	Microsoft-Windows-Security-
	183	[ ]	183	183	2023-06-28 16...	8224	Info	VSS
	184	[ ]	184	184	2023-06-28 16...	16394	Info	Microsoft-Windows-Security-
	185	[ ]	185	185	2023-06-28 16...	1034	Info	Microsoft-Windows-Security-
	186	[ ]	186	186	2023-06-28 16...	1033	Info	Microsoft-Windows-Security-
	187	[ ]	187	187	2023-06-28 16...	16384	Info	Microsoft-Windows-Security-
	188	[ ]	188	188	2023-06-28 16...	1001	Info	Windows Error Reporting
	189	[ ]	189	189	2023-06-28 16...	15	Info	SecurityCenter
	190	[ ]	190	190	2023-06-28 17...	16394	Info	Microsoft-Windows-Security-
	191	[ ]	191	191	2023-06-28 17...	16384	Info	Microsoft-Windows-Security-
	192	[ ]	192	192	2023-06-28 17...	1001	Info	Windows Error Reporting
	193	[ ]	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

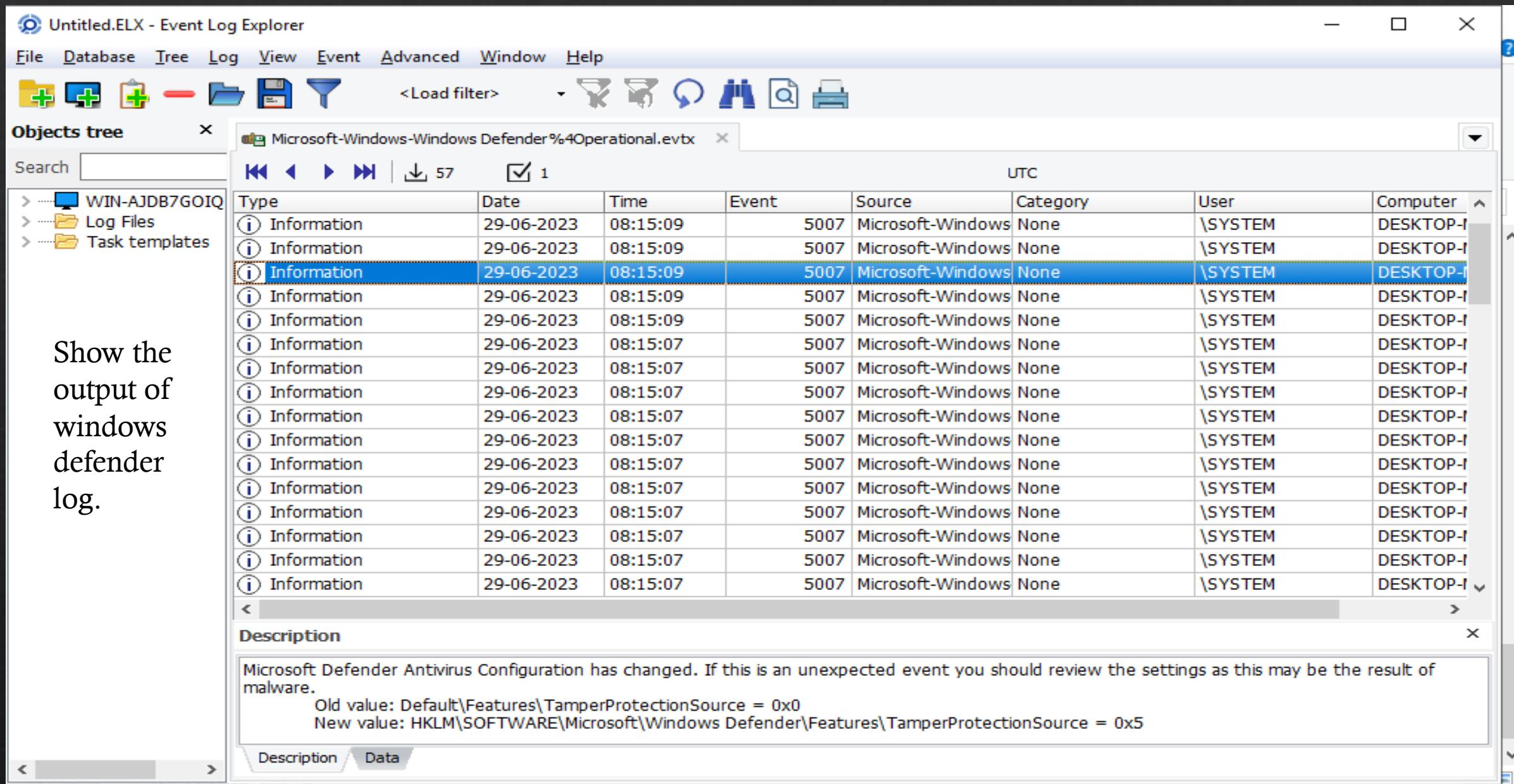
5001

Defender disabled

The screenshot shows the Windows Event Log Explorer interface. The left sidebar displays a navigation tree with categories like Pictures, Evidence, Execution, NTFS, Registry, This PC, 3D Objects, Desktop, Documents, Downloads, Music, Pictures, Videos, and drives SDT\_x64FREE\_EN, CD Drive (D:), System Reserved, Local Disk (F:), and Local Disk (G:). The main pane lists event logs from the 'logs' folder under 'SDT\_x64FREE\_EN-EN-US\_VHD (C:) > Cases > F > Windows > System32 > winevt'. The events are sorted by date modified. The event with ID 5000, titled 'Microsoft-Windows-Windows Defender...', is highlighted with a blue selection bar. Other event logs listed include Microsoft-Windows-UserPnp%4DeviceIn..., Microsoft-Windows-VolumeSnapshot-Dr..., Microsoft-Windows-Wcmsvc%4Operatio..., Microsoft-Windows-WebAuthN%4Opera..., Microsoft-Windows-WER-PayloadHealth..., Microsoft-Windows-WFP%4Operational, Microsoft-Windows-Windows Defender..., Microsoft-Windows-Windows Defender..., Microsoft-Windows-Windows Firewall W..., Microsoft-Windows-Windows Firewall W..., Microsoft-Windows-WindowsBackup%4..., Microsoft-Windows-WindowsUpdateClie..., Microsoft-Windows-WinINet-Config%4P..., Microsoft-Windows-Winlogon%4Operati..., Microsoft-Windows-WinRM%4Operatio..., Microsoft-Windows-WMI-Activity%4Op..., Security, Setup, and System. The status bar at the bottom indicates '101 items' and '1 item selected 68.0 KB'. The system tray at the bottom right shows the date and time as '16-07-2023 12:40'.

Name	Date modified	Type	Size
Microsoft-Windows-UserPnp%4DeviceIn...	28-06-2023 16:31	Event Log	68 KB
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
<b>Microsoft-Windows-Windows Defender...</b>	<b>29-06-2023 09:07</b>	<b>Event Log</b>	<b>68 KB</b>
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

Load the Windows  
Defender log on  
Event Log Explorer



12:41  
16-07-2023



Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

<Load filter>

Objects tree

Search

Microsoft-Windows-Windows Defender%4Operational.evtx

Type Date Time Event Source Category User Computer

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



12:46  
16-07-2023

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

<Load filter>

Objects tree 57 1 UTC

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

Windows Search File Explorer Internet Explorer Firefox Task Manager Event Viewer Control Panel 12:45 16-07-2023

## 2. System log Analysis

Source  
System

Event IDs      Description  
7045            A new service was installed

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

- File Explorer Title Bar:** logs
- Menu Bar:** File, Home, Share, View
- Toolbar:** 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, Select all, Select none, Invert selection.
- Breadcrumb Navigation:** This PC > SDT\_x64FREE\_EN-US\_VHD (C:) > Cases > F > Windows > System32 > winevt > logs
- Search Bar:** Search logs
- Left Sidebar:** Navigation pane with links: Pictures, Evidence, Execution, NTFS, Registry, This PC, 3D Objects, Desktop, Documents, Downloads, Music, Pictures, Videos, SDT\_x64FREE\_EN, CD Drive (D:), System Reserved, Local Disk (F:), Local Disk (G:).
- Table View:** A list of event logs in the logs folder. The table has columns: Name, Date modified, Type, Size. The "System" log file is selected and highlighted.

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
<b>System</b>	29-06-2023 09:07	Event Log	1,092 KB
Windows PowerShell	29-06-2023 09:07	Event Log	1,092 KB

**Bottom Status Bar:** 101 items, 1 item selected, 1.06 MB

**Taskbar:** Icons for File Explorer, Edge, Firefox, File Manager, Task View, Taskbar settings, Volume, Brightness, and Date/Time (13:06, 16-07-2023).

**Text Overlay:** Lod the system log on Event log explorer

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree  <Load filter>     

System.evtx

Search

Type Date Time Event Source Category User

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

Click this icon 

Description

DHCPv4 client service is stopped. ShutDown Flag value is 1

Description Data





&lt;Load filter&gt;



## Objects tree

Search

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

## System.evtx

◀ ▶ ⏪ ⏩ ⏴ 818 ⏷ 10  UTC

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

13:05  
16-07-2023

### 3. Security and Authentication Event logs

Source

Security

Event IDs

4624

Description

An account was successfully logged on

The screenshot shows a Windows File Explorer window with the following path: This PC > SDT\_x64FREE\_EN-US\_VHD (C:) > Cases > F > Windows > System32 > winevt > logs. The left sidebar shows standard folder icons like Pictures, Evidence, Execution, etc. The main pane displays a list of event log files. The file 'Security' is highlighted with a blue selection bar at the bottom. The columns in the list view are Name, Date modified, Type, and Size.

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

Click the security event log and load on the event explorer



## Objects tree

Search

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

Click this icon for filter the event id

&lt; Load filter&gt;



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

## Description

An account was successfully logged on.

Subject:



Fill the event id and description as per requirement

Untitled.ELX - Event Log Explorer

File Database Tree Log

Objects tree

Search WIN-AJDB7GOIQ Log Files Task templates

Event types

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

Apply filter to:

Active event log view (File: C:\Cases\F\Windows\System32\winevt\logs\Security.evtx)

Event log view(s) on your choice

Source: Category: User: Computer:

Event ID(s): 4624

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)

Date Time Separately

From: 17-07-2023 To: 17-07-2023

Display event for the last 0 days 0 hours

Custom columns Description params

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

OK Cancel

Computer DESKTOP-MD2H1 DESKTOP-MD2H1 DESKTOP-MD2H1 DESKTOP-MD2H1 DESKTOP-MD2H1 DESKTOP-MD2H1



05:40

17-07-2023





&lt;Load filter&gt;



## 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-MD2H0
Audit Success	29-06-2023	08:46:45	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H0
Audit Success	29-06-2023	08:32:32	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H0
Audit Success	29-06-2023	08:27:36	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H0
Audit Success	29-06-2023	08:16:45	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H0
Audit Success	29-06-2023	08:14:34	4624	Microsoft-Windows	Logon	N/A	DESKTOP-MD2H0

## Description

An account was successfully logged on.

## Subject:

Security ID: S-1-5-18  
Account Name: DESKTOP-MD2HCP T\$  
Account Domain: WORKGROUP  
Logon ID: 0x3e7

## Logon Information:

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

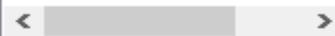
## Impersonation Level:

Impersonation

## New Logon:

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

Show the all detail about this event log.

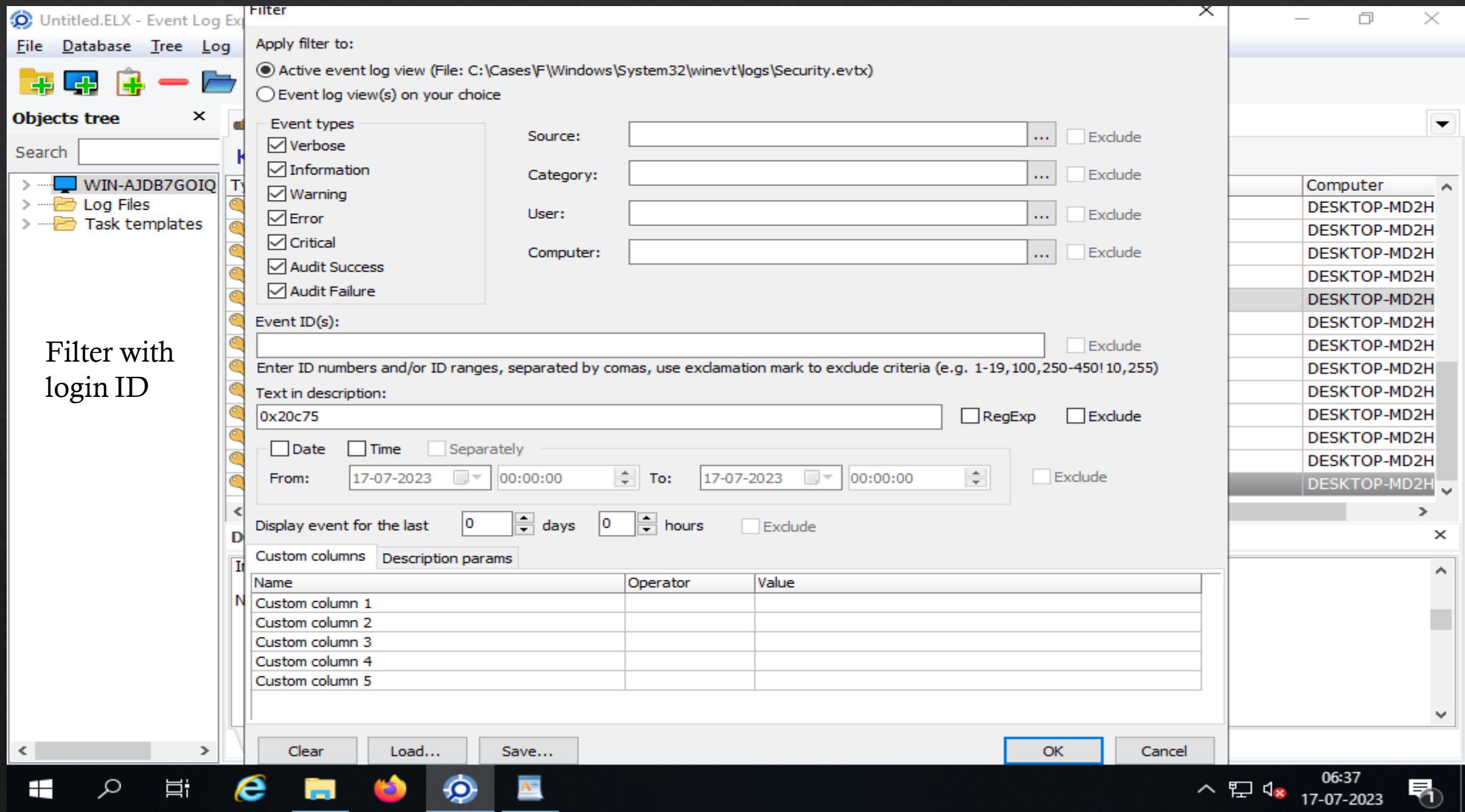


Description

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 View Event Advanced Window Help

Objects tree x

Search

WIN-AJDB7GOIQ

Log Files

Task templates

Same login ID and details show different

< Load filter > x

Security.evtx x

1161 19  1 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	16:19:19	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 x

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.

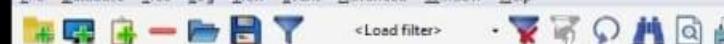
Description Data



06:21 17-07-2023

## Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help



## 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

Same login  
ID and  
details show  
different

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

## 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: 0x45za

## New Account:

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

## Attributes:

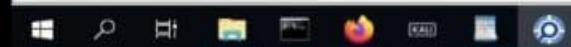
SAM Account Name: art-test  
 Display Name: <value not set>  
 User Principal Name: -  
 Home Directory: <value not set>  
 Home Drive: <value not set>  
 Script Path: <value not set>  
 Profile Path: <value not set>  
 User Workstations: <value not set>  
 Password Last Set: <never>  
 Account Expires: <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.

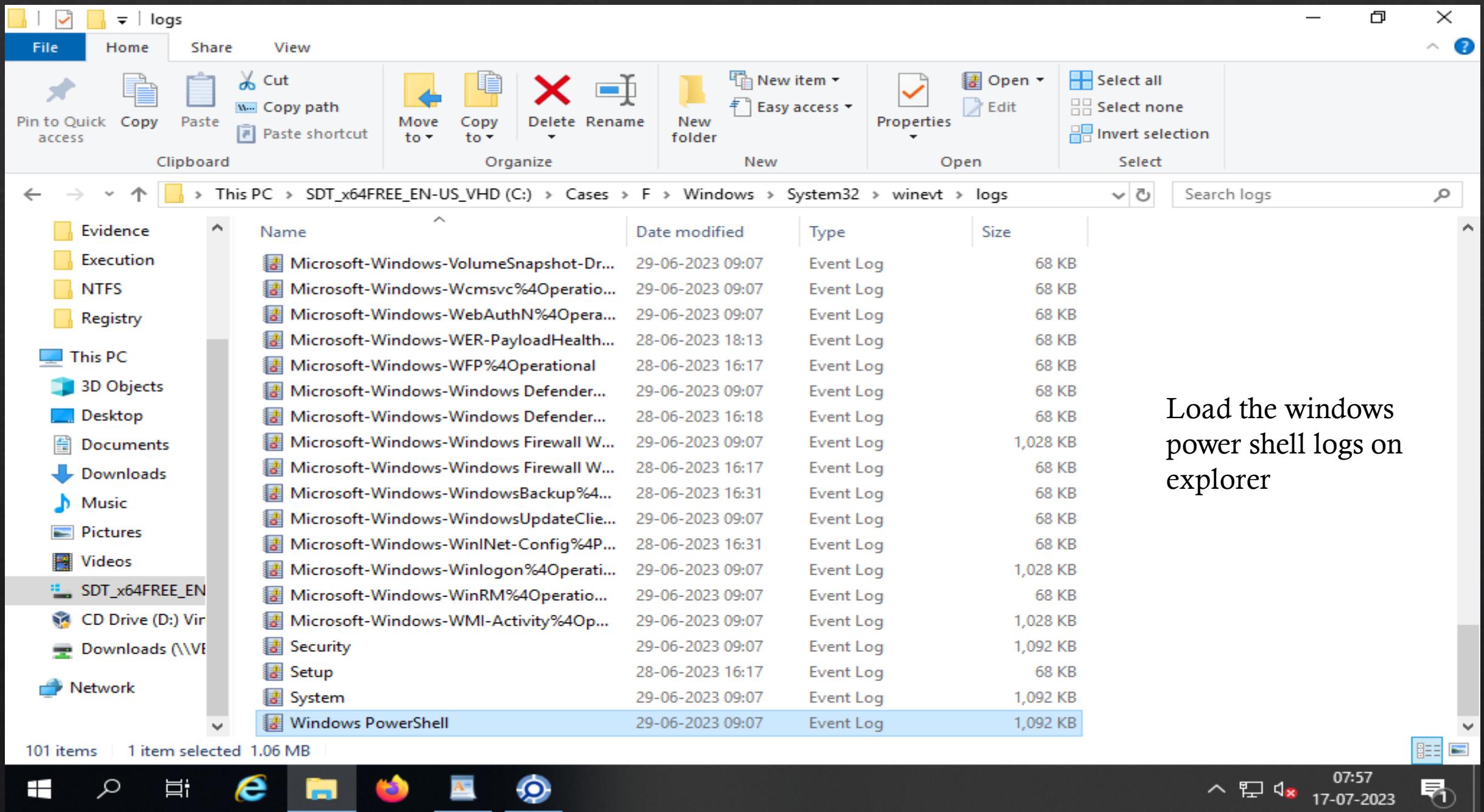
7:29 PM Cloud  
5/16/2022

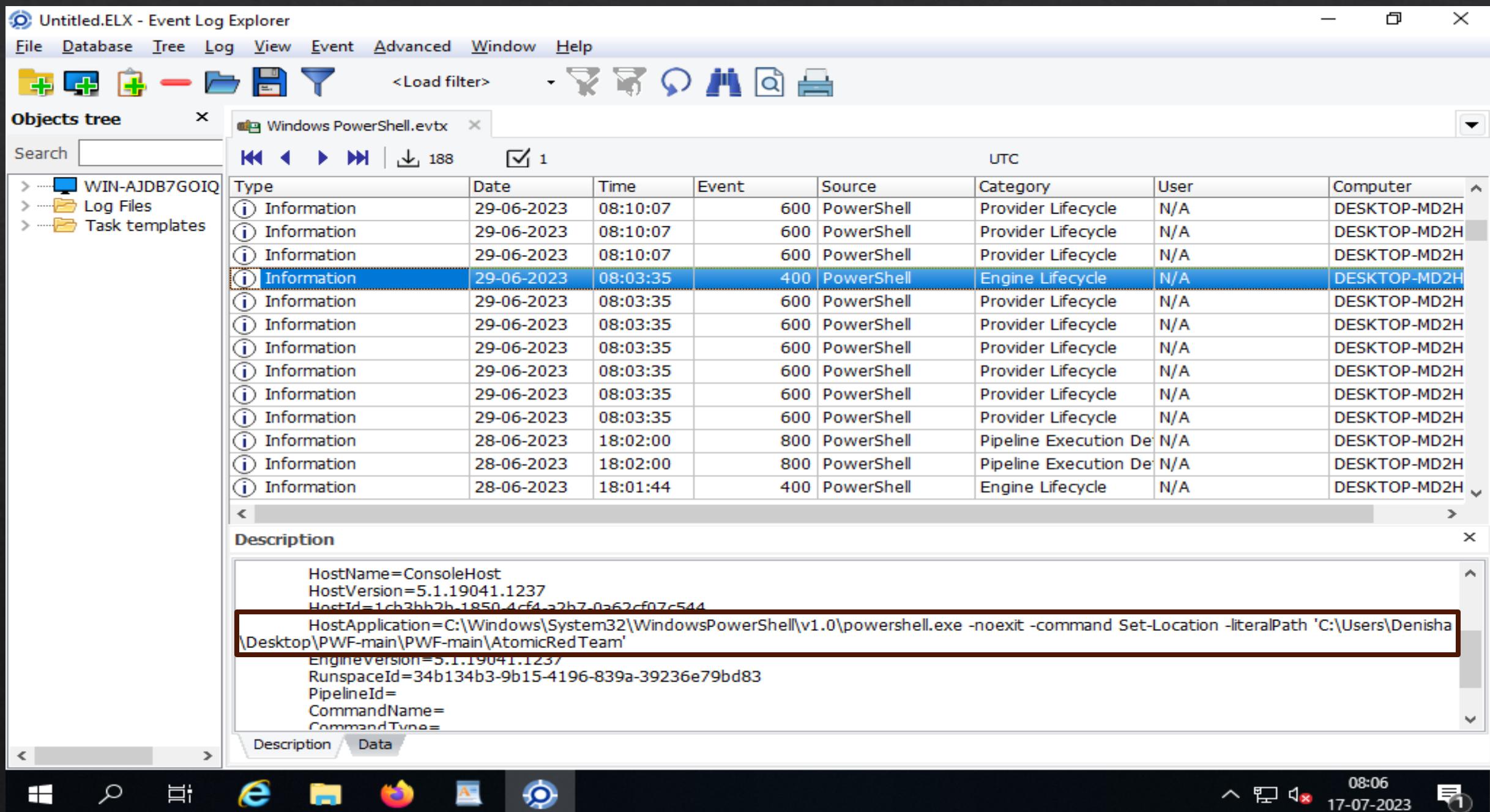
## 5. Windows Event logs Power shell overview, Analyse Malicious Activity.

Source  
Windows PowerShell

Event IDs	Description
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.







&lt;Load filter&gt;



## Objects tree

Search

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

Windows PowerShell.evtx

Back Forward Download 188  1

UTC

Type	Date	Time	Event	Source	Category	User	Computer
(i) Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
(i) Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
(i) Information	29-06-2023	08:10:07	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
(i) Information	29-06-2023	08:03:35	400	PowerShell	Engine Lifecycle	N/A	DESKTOP-MD2H
(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
(i) Information	29-06-2023	08:03:35	600	PowerShell	Provider Lifecycle	N/A	DESKTOP-MD2H
(i) Information	28-06-2023	18:02:00	800	PowerShell	Pipeline Execution De	N/A	DESKTOP-MD2H
(i) Information	28-06-2023	18:02:00	800	PowerShell	Pipeline Execution De	N/A	DESKTOP-MD2H
(i) 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=r8d3a583-872c-4d21-hf69-5e941e11h7d6
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

08:07  
17-07-2023

# 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.



Recyclable

forensic@WIN-AJDB7GOIOEJ: ~

Try: sudo apt install <deb name>

```
forensic@WIN-AJDB7GOIQEJ:~$ sudo apt-get update
[sudo] password for forensic:
FirGet: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]
EvenGet:7 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [367 kB]
ExpGet: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]
NoteGet: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]
bcGet: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]
```

Windows Server 2019 Datacenter Evaluation

Windows License valid for 156 days

Build 17763.rs5\_release.180914-1434



Recycle Bin

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 bzr 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.
After this operation, 228 MB of additional disk space will be used.
```

accounts\_V...

Windows Server 2019 Datacenter Evaluation  
Windows License valid for 156 days  
Build 17763.rs5\_release.180914-1434

17:41 21-07-2023

```
Recycle Bin  forensic@WIN-AJDB7GOIQEJ: ~
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.
  --isolated           Run pip in an isolated mode, ignoring environment variables and user configuration.

Windows Server 2019 Datacenter Evaluation
Windows License valid for 156 days
Build 17763.rs5_release.180914-1434
17:47  21-07-2023  1
```

```
--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.manylinux_2_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:~$
```

accounts\_V...

Windows Server 2019 Datacenter Evaluation  
Windows License valid for 156 days  
Build 17763.rs5\_release.180914-1434



17:50 21-07-2023 1

```
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

## 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-AJDB7GOIQUEJ:/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-AJDB7GOIQUEJ:~$ pwd
/home/forensic
forensic@WIN-AJDB7GOIQUEJ:~$ cd /mnt
forensic@WIN-AJDB7GOIQUEJ:/mnt$ ls
c
forensic@WIN-AJDB7GOIQUEJ:/mnt$ cd ..
forensic@WIN-AJDB7GOIQUEJ:$ 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-AJDB7GOIQUEJ:$ cd /mnt/c/Cases/Analysis/Memory/
forensic@WIN-AJDB7GOIQUEJ:/mnt/c/Cases/Analysis/Memory$ pwd
/mnt/c/Cases/Analysis/Memory
forensic@WIN-AJDB7GOIQUEJ:/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-AJDB7GOIQUEJ:/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.



08:12  
22-07-2023

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

```
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.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.joblinks.JobLinks
    Print process job link information
```

we have use  
windows info  
plugins .



08:12  
22-07-2023

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



```
Progress: 99.98      Reading Symbol layer
Progress: 99.98      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
898BF862997-1.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 TimeStamp     Wed Jan  4 04:27:11 1995
```

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



Type this command how the  
result.



08:29  
22-07-2023

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

```
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 TimeStamp      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

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



09:34  
22-07-2023

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

596      512      winlogon.exe      0xcc068a750240  6      -      1      False      2023-07-22 06:33:37.000000      N/A      Disab
led
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$
```



09:34  
22-07-2023

```

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 | Memory

File Home Share View

Pin to Quick access Copy Paste Cut Copy path Paste shortcut Clipboard

Move Copy Delete Rename New New item Easy access Properties Open Edit Select all Select none

dll - Notepad

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.exe		
winlogon.exe	0x7ff942430000	0x1f5000		ntdll.dll	C:\Windows\SYSTEM32\ntdll.dll	
winlogon.exe	0x7ff941f10000	0xbe000	KERNEL32.DLL	C:\Windows\System32\KERNEL32.DLL		
winlogon.exe	0x7ff93fe70000	0x2c9000		KERNELBASE.dll	C:\Windows\System32\KERNELBASE.dll	
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\RPCRT4.dll	
winlogon.exe	0x7ff940630000	0x355000		combase.dll	C:\Windows\System32\combase.dll	
winlogon.exe	0x7ff940210000	0x100000		ucrtbase.dll	C:\Windows\System32\ucrtbase.dll	
winlogon.exe	0x7ff9412f0000	0xac000	advapi32.dll	C:\Windows\System32\advapi32.dll		
winlogon.exe	0x7ff93f9c0000	0x4b000	powrprof.dll	C:\Windows\SYSTEM32\powrprof.dll		
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	0x1a100		user32.dll	C:\Windows\System32\user32.dll	
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\gdi32full.dll	
winlogon.exe	0x7ff940140000	0x9d000	msvcp_win.dll	C:\Windows\System32\msvcp_win.dll		
winlogon.exe	0x7ff942290000	0x30000	IMM32.DLL	C:\Windows\System32\IMM32.DLL		
winlogon.exe	0x7ff93f890000	0x5a000	winsta.dll	C:\Windows\SYSTEM32\winsta.dll		

All dll file here.

3 items | 1 item selected 5.66 KB

Unix (LF) Ln 1, Col 1 100%

12:38 22-07-2023

File Home Share View

Pin to Quick access Copy Paste Cut Copy path Paste shortcut Clipboard

Move Copy Delete Rename New New item Easy access Properties Open Edit Select all Select none

dll - Notepad

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.exe		
winlogon.exe	0x7ff942430000	0x1f5000		ntdll.dll	C:\Windows\SYSTEM32\ntdll.dll	
winlogon.exe	0x7ff941f10000	0xbe000	KERNEL32.DLL	C:\Windows\System32\KERNEL32.DLL		
winlogon.exe	0x7ff93fe70000	0x2c9000		KERNELBASE.dll	C:\Windows\System32\KERNELBASE.dll	
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\RPCRT4.dll	
winlogon.exe	0x7ff940630000	0x355000		combase.dll	C:\Windows\System32\combase.dll	
winlogon.exe	0x7ff940210000	0x100000		ucrtbase.dll	C:\Windows\System32\ucrtbase.dll	
winlogon.exe	0x7ff9412f0000	0xac000	advapi32.dll	C:\Windows\System32\advapi32.dll		
winlogon.exe	0x7ff93f9c0000	0x4b000	powrprof.dll	C:\Windows\SYSTEM32\powrprof.dll		
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	0x1a100		user32.dll	C:\Windows\System32\user32.dll	
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\gdi32full.dll	
winlogon.exe	0x7ff940140000	0x9d000	msvcp_win.dll	C:\Windows\System32\msvcp_win.dll		
winlogon.exe	0x7ff942290000	0x30000	IMM32.DLL	C:\Windows\System32\IMM32.DLL		
winlogon.exe	0x7ff93f890000	0x5a000	winsta.dll	C:\Windows\SYSTEM32\winsta.dll		

All dll file here.

3 items | 1 item selected 5.66 KB

Unix (LF) Ln 1, Col 1 100%

12:38 22-07-2023

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

## 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 06:33:37.0		
:33:37.000000	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		
:33:37.000000	pid.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	



12:45  
22-07-2023

Memory

File Home Share View

Pin to Quick access Copy Paste Cut Copy path Move to Copy to Delete Rename New folder New item Easy access Properties Open Select all Select none Invert selection

Clipboard Organize New Open Select

← → ↑ This PC > SDT\_x64FREE\_EN-US\_VHD (C:) > Cases > Analysis > Memory Search Memory

Evidence Execution Memory Registry This PC 3D Objects Desktop Documents Downloads Music Pictures Videos SDT\_x64FREE\_EN CD Drive (D:) Virtual Drives Downloads (\\\) Network

Name Date modified Type Size

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.fwbase.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

50 items | 1 item selected 5.66 KB

12:45 22-07-2023

Show the all dump file in memory folder

```
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.
```

# Identify process owners and associated SIDs

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

```
forensic@WIN-AJDB7GOIQUEJ:/mnt/c/Cases/Analysis/Memory
TTBL
TEMP
TEMPP
H7^A
TEMP$  
TEMP
TEMP
TEMPd
iv01
TEMP
g=z=
TEMP
forensic@WIN-AJDB7GOIQUEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.getsids -h
Volatility 3 Framework 2.4.1
usage: volatility windows.getsids.GetIDs [-h] [--pid [PID [PID ...]]]

optional arguments:
  -h, --help            show this help message and exit
  --pid [PID ...]       Filter on specific process IDs
forensic@WIN-AJDB7GOIQUEJ:/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-AJDB7GOIQUEJ:/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] [--reurse]

optional arguments:
-h, --help      show this help message and exit
--offset OFFSET Hive Offset
--key KEY       Key to start from
--reurse        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_neu
tral_cw5n1h2txyewy\ActivationStore.dat  Disabled
0xa30317586000  \??\C:\Users\Denisha\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\Settings\settings.dat  D
isabled
0xa303177b6000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.StartMenuExperienceHost_10.0.19
041.1023_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat  Disabled
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.registry.printkey --offset 0xa30314774
000 --key AtomicRedTeam
```

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

```
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

## 3. Run Tools

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

## 2. Prepare Evidence

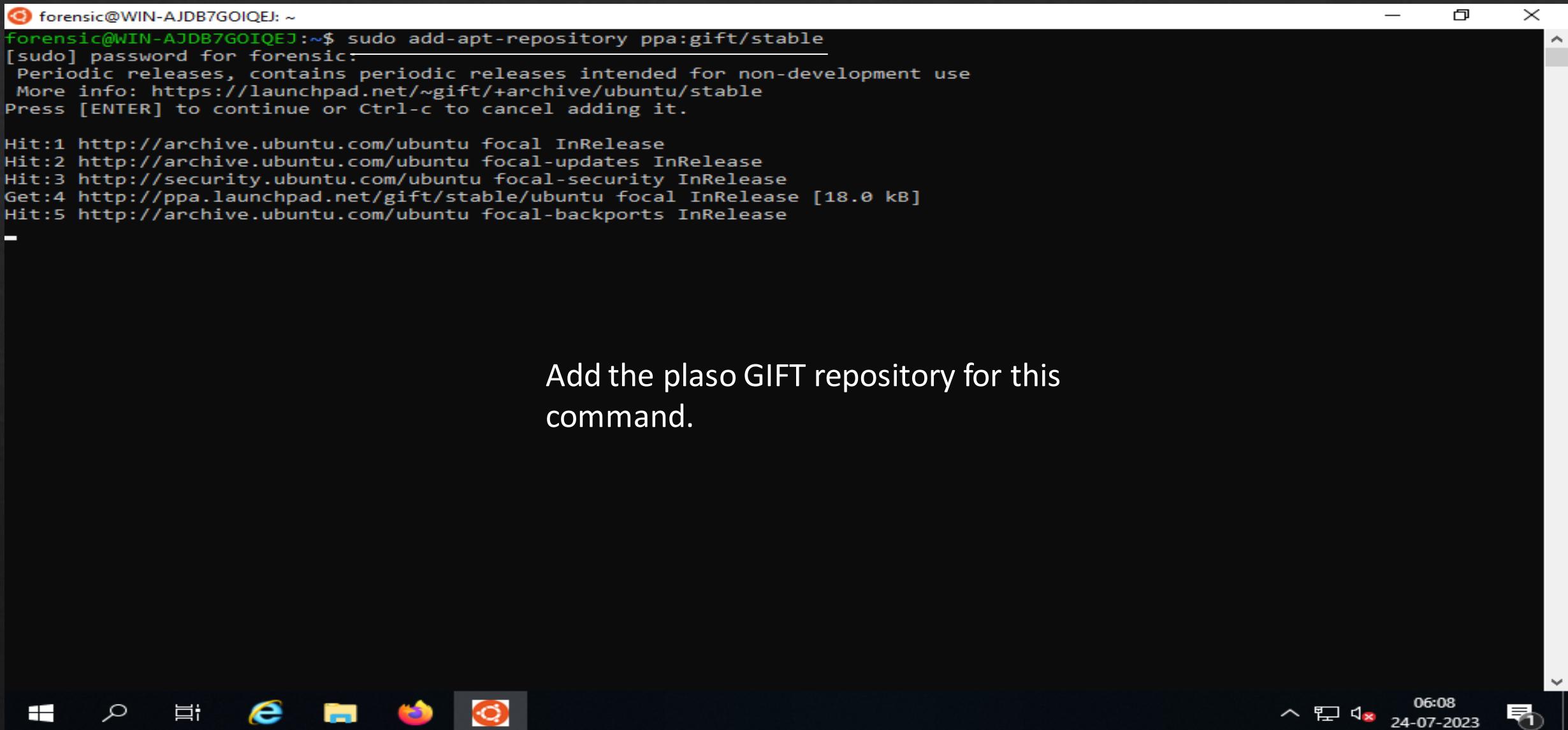
Disk image(RAW!)  
Memory image

## 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.

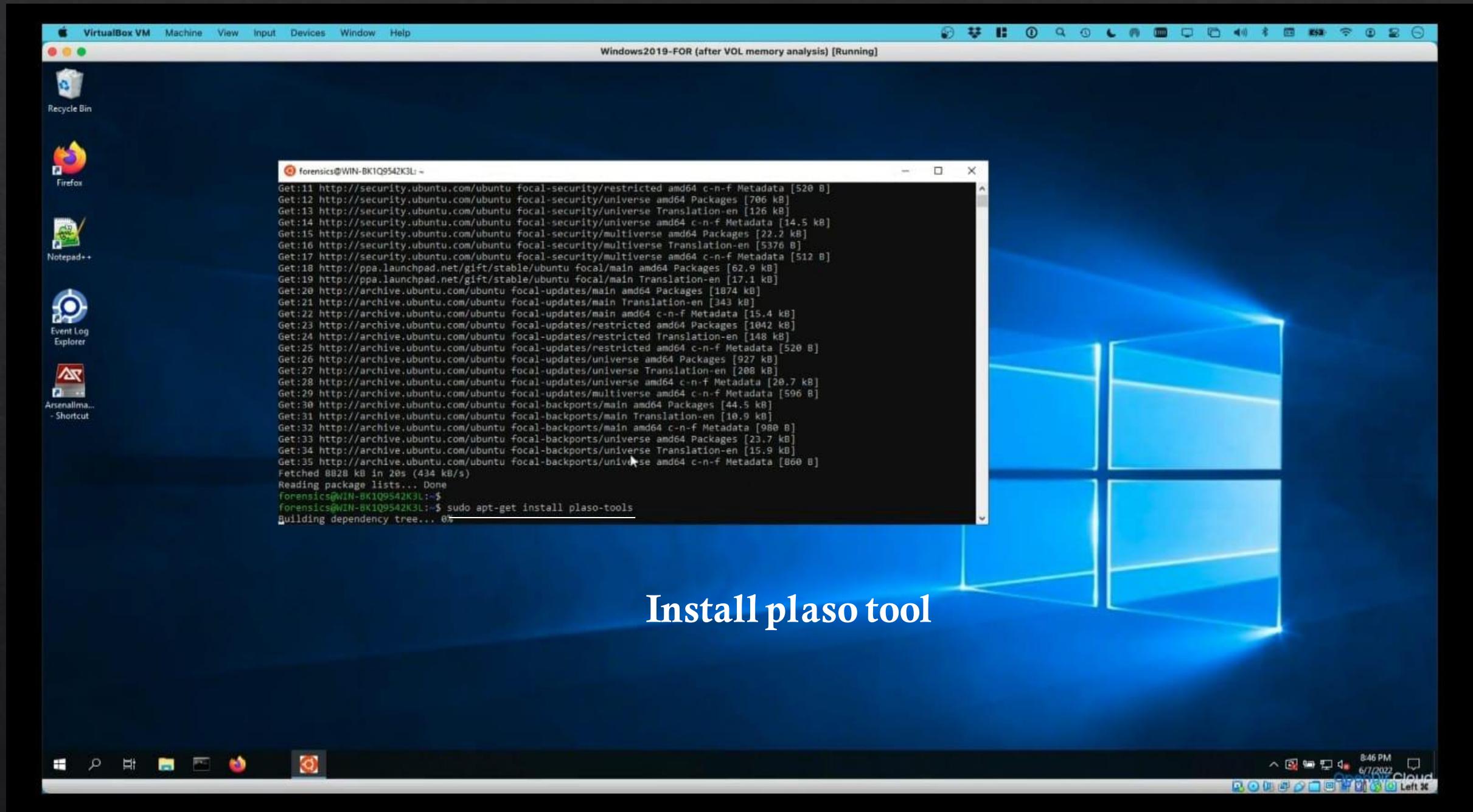
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu focal-security InRelease
Get:4 http://ppa.launchpad.net/gift/stable/ubuntu focal InRelease [18.0 kB]
Hit:5 http://archive.ubuntu.com/ubuntu focal-backports 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 1



# Install plaso tool

File Home Share View Disc Image Tools Manage Evidence

Pin to Quick access Copy Paste Cut Copy path Move to Copy to Delete Rename New folder New item Open New Open Select all Select none Invert selection

Clipboard Organize New Select

← → ↑ This PC > Downloads (\VBoxSrv) (Z:) > Evidence Search Evidence

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

Evidence Execution NTFS Registry This PC 3D Objects Desktop Documents Downloads Music Pictures Videos SDT\_x64FREE\_EN CD Drive (D:) Virtual Machine Downloads (\VBoxSrv) Network

Target Machine Virtual Hard disk copy

1 item | 1 item selected 13.3 GB



14:18  
24-07-2023

Cases

File Home Share View

Pin to Quick access Copy Paste Cut Copy path Move to Copy to Delete Rename New folder New item Open Easy access Properties Select all Select none Invert selection

Clipboard Organize New Open Select

Back Forward Up This PC SDT\_x64FREE\_EN-US\_VHD (C:) Cases Search Cases

Name	Date modified	Type	Size
Evidence			
Execution			
NTFS			
Registry			
This PC			
3D Objects			
Desktop			
Documents			
Downloads			
Music			
Pictures			
Videos			
SDT_x64FREE_EN			
CD Drive (D:) Vir			
Downloads (\\\V)			
Network			

Paste here the hard disk.

6 items

17:42  
24-07-2023



Recycle Bin



Firefox



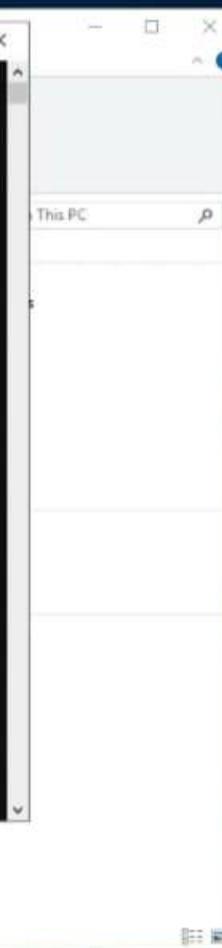
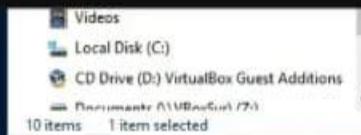
Notepad++

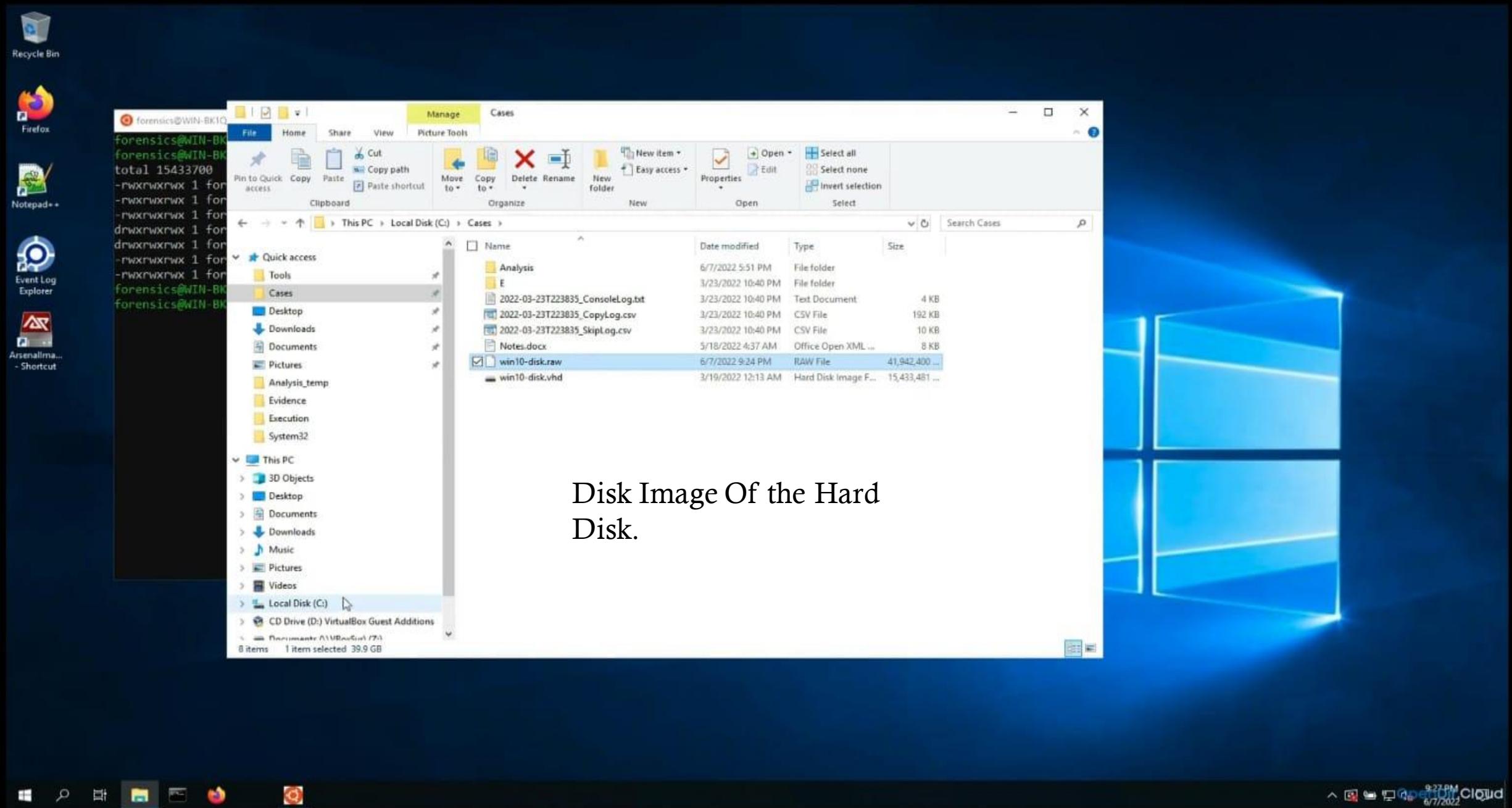
Event Log  
ExplorerArsenal mal...  
- Shortcut

```
forensics@WIN-BK1Q9542K3L:/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 .malysis  
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

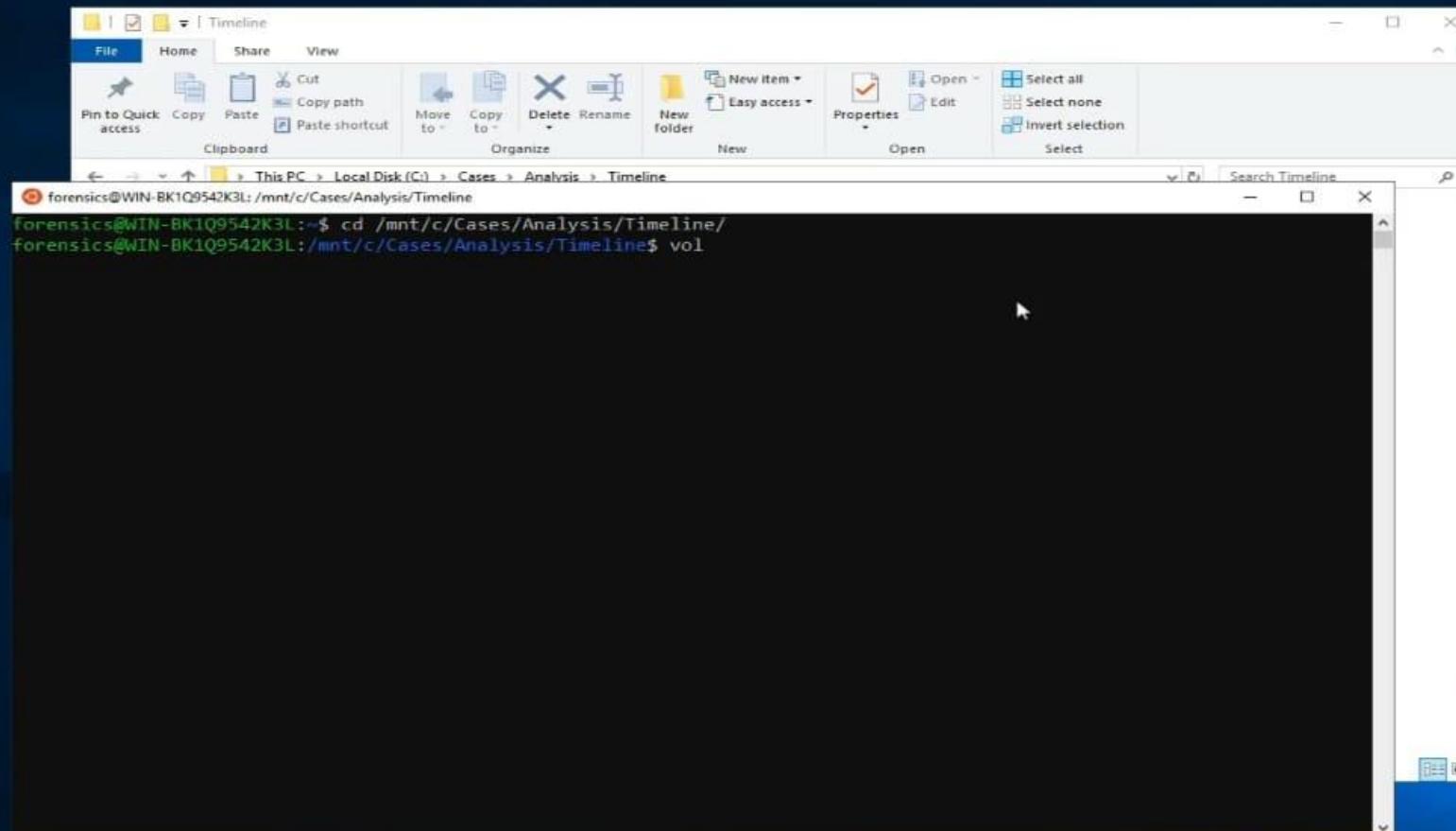
Using the Following Command  
converting the disk image.





# Memory timeline creation with Volatility3

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





Recycle Bin



Firefox



Notepad++

Event Log  
ExplorerArsenalma...  
- Shortcut

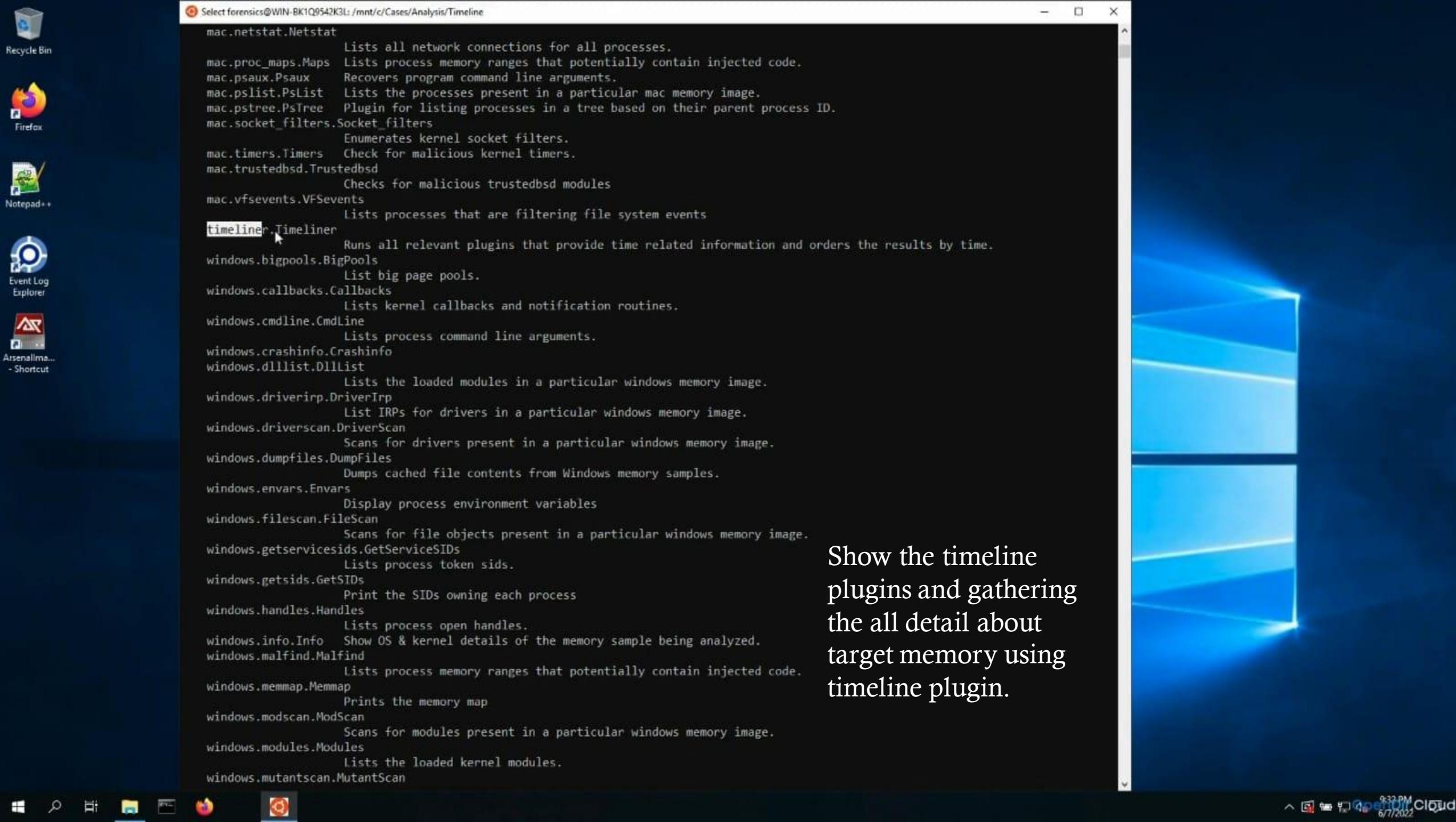
The screenshot shows a Windows desktop environment. In the center, there is a terminal window titled 'Timeline' with the following command history:

```
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
```

To the right of the terminal window, a File Explorer window is open, showing the path 'This PC > Local Disk (C:) > Cases > Analysis > Timeline'. The File Explorer interface includes a ribbon bar with 'File', 'Home', 'Share', and 'View' tabs, and various toolbar icons for file operations like Cut, Copy, Paste, Delete, and New.

Using vol -h show all  
plugins in detail.





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

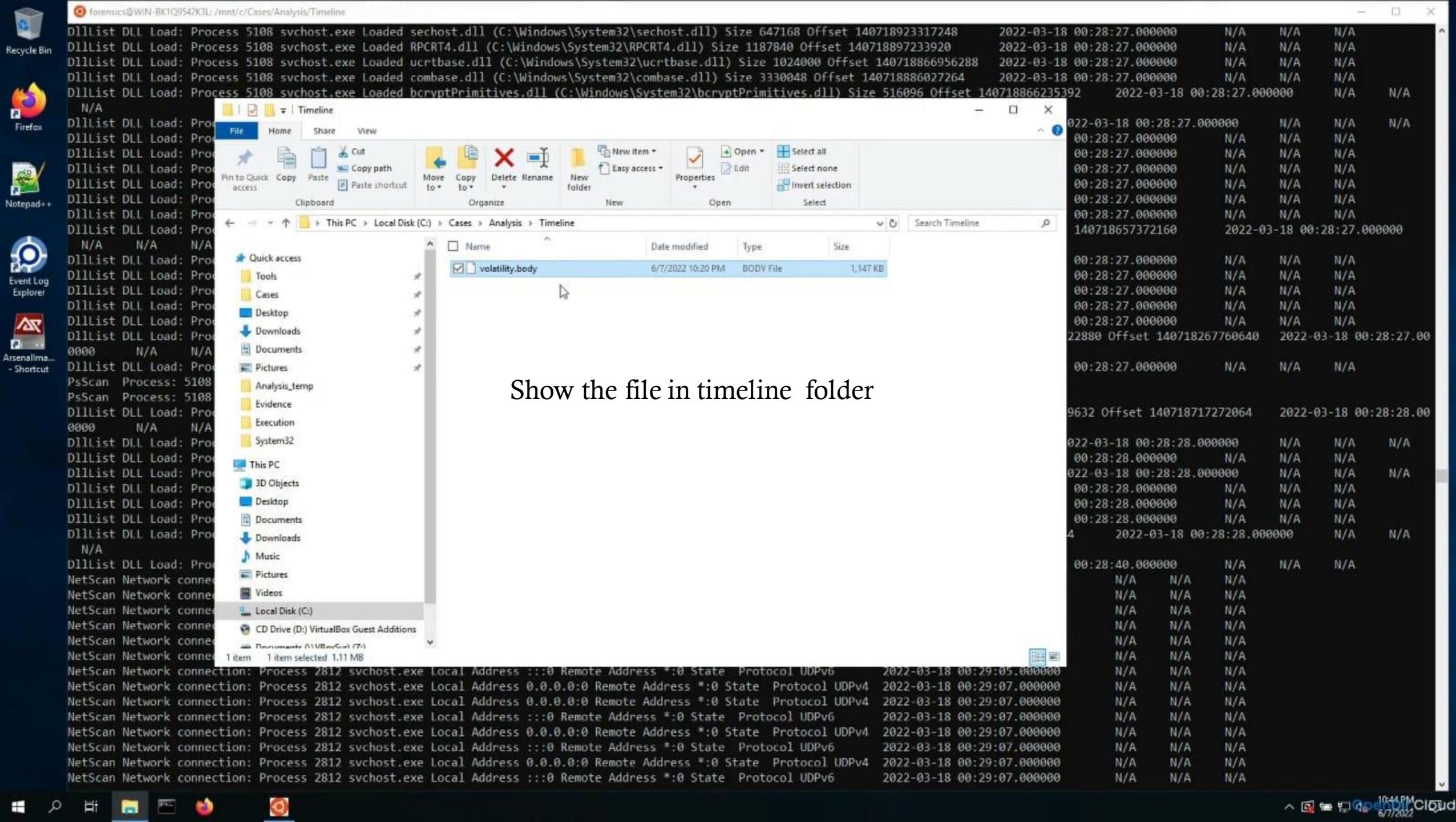
```
Recycle Bin
Firefox
Notepad++
Event Log Explorer
ArsenalIma...
- Shortcut

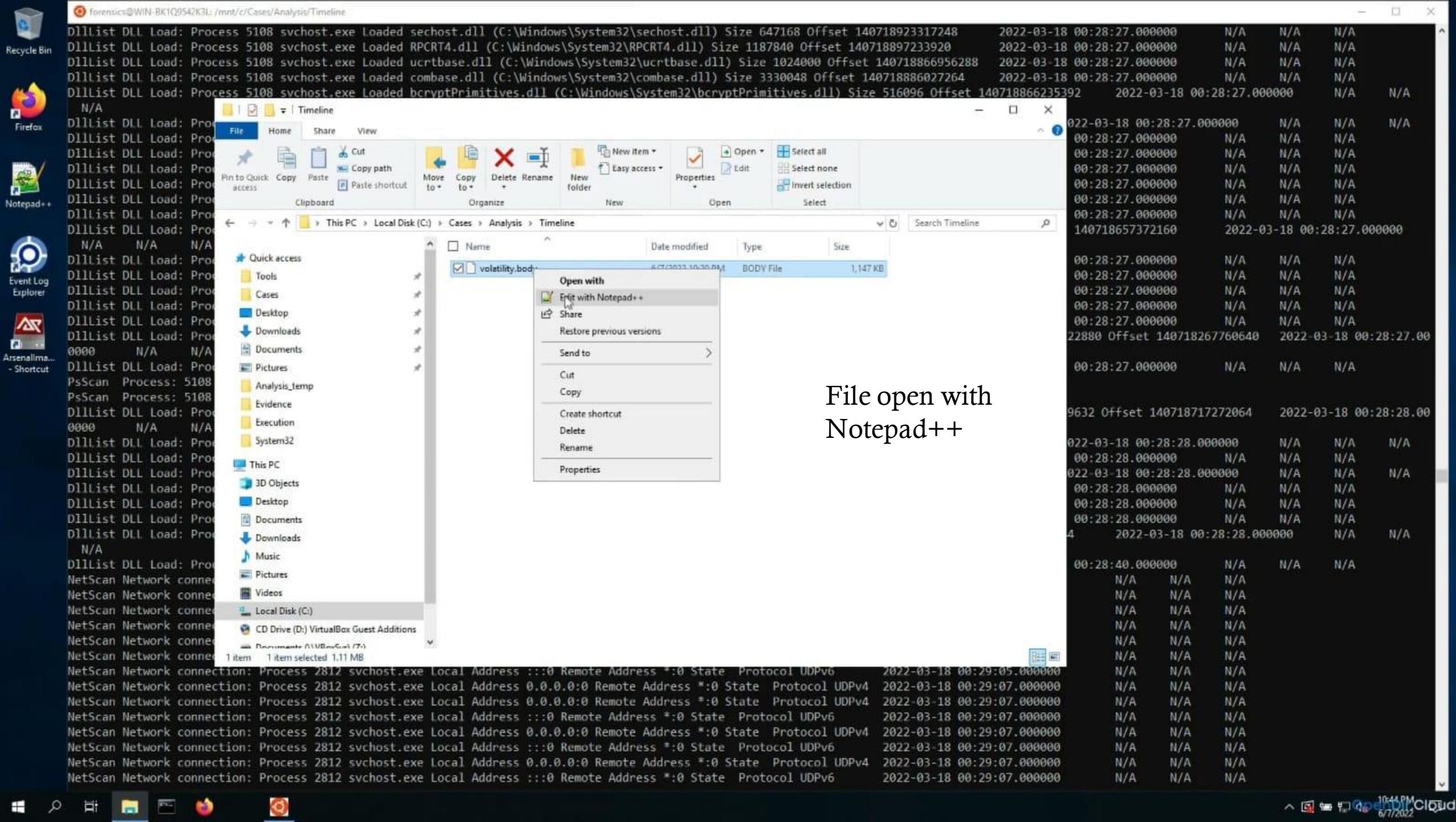
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline
  windows.registry.certificates.Certificates
    Lists the certificates in the registry's Certificate Store.
  windows.registry.hivelist.HiveList
    Lists the registry hives present in a particular memory image.
  windows.registry.hivescan.HiveScan
    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.ssdt.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$ 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.





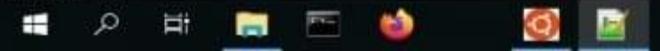


```

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

```
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$ 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



Arsenalma...

- 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.



7:30 AM 6/8/2022 OpenCloud



Particular Bias



Firefox



Notebooks



## Event Log



### Arsenolima.

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

plaso - log2timeline version 2022042

Source path : /mnt/c/Cases/win10-disk.ra  
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\edbres0002.irs

Processing completed.

Number of warnings generated while extracting events: 9

Use `pinfp` 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.paso
-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$ pinfo nv disk.paso
```

```
*****  
Plaso Storage Information  
*****  
  Filename : disk.palo  
  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.



Recycle Bin



```
***** 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.



2:43 AM 6/8/2022 OpenCloud

# 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.paso
-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.paso 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

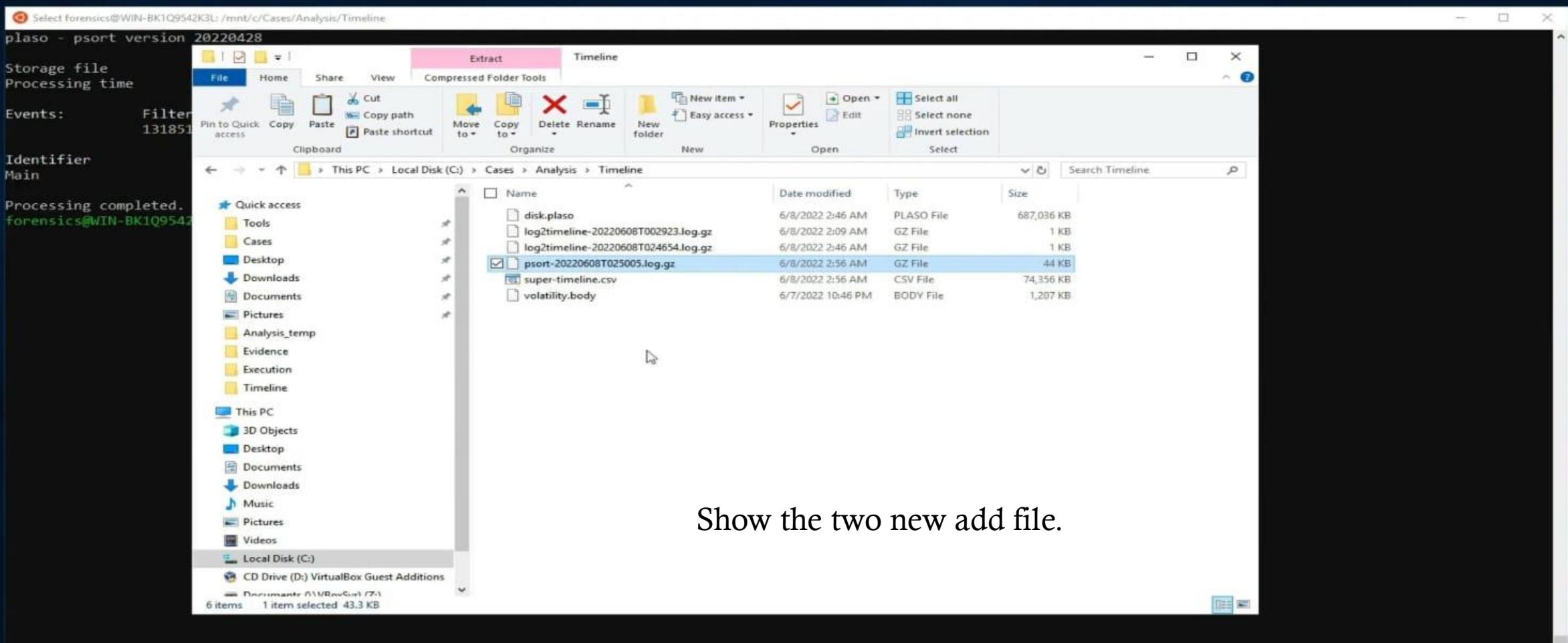
Source path      : /mnt/c/Cases/Analysis/Timeline/volatility.body
Source type     : single file
Processing time : 00:00:02

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'"
```

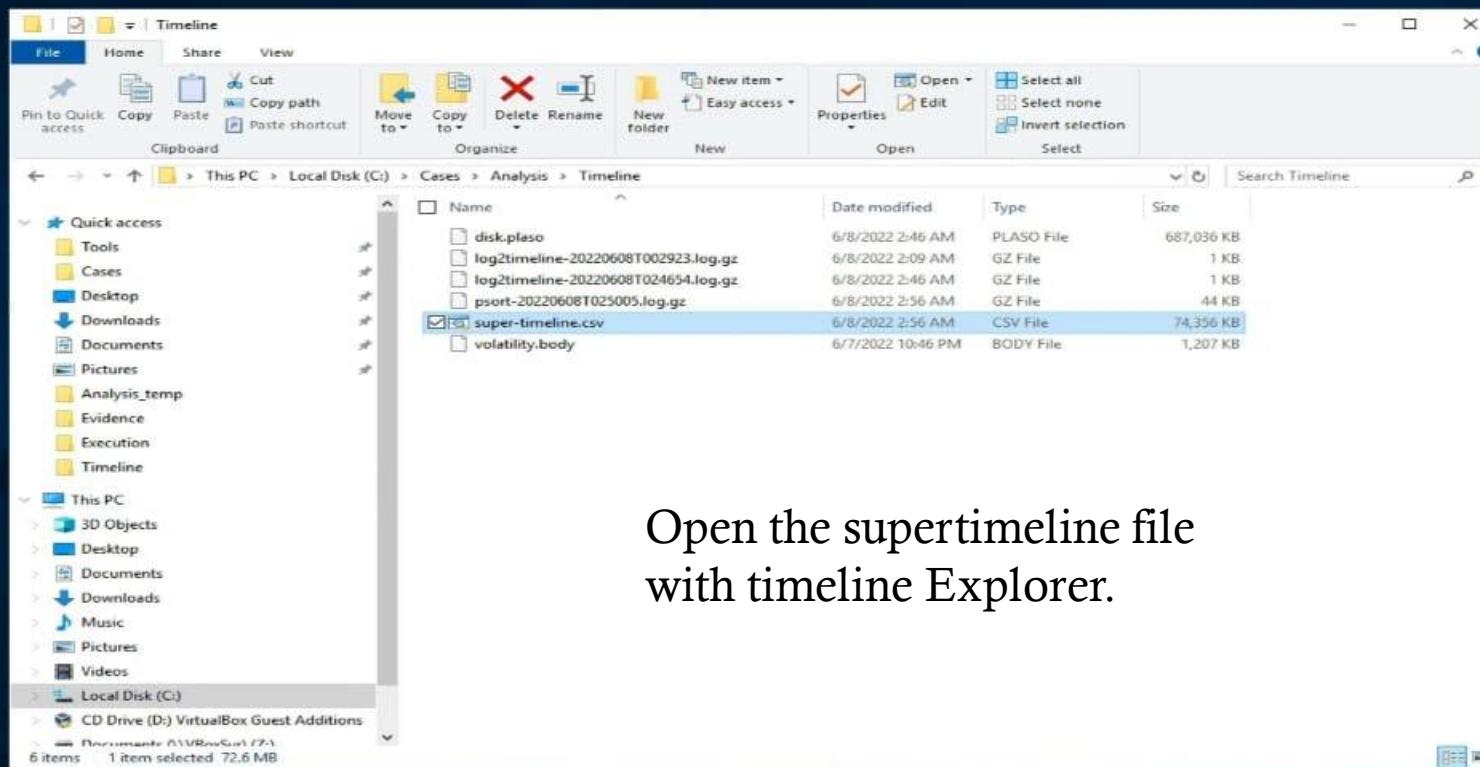
Using this command plaso file convert to csv file. And also create super timeline.



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
T	-	-	-	-	-	-	-
915	<input type="checkbox"/>	2001-01-01 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.



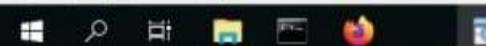
Drag a column header here to group by that column

Enter text to search...

Find

Line	Tag	Timestamp	Source Description	Source Name	macb	Inode	Long Description
66		2022-03-01 22:14:48	PE Event	PE	...b	127091	PE Type: Dynamic Link Library (DLL)
67		2022-03-01 22:14:49	PE Event	PE	...b	127093	PE Type: Dynamic Link Library (DLL)
68		2022-03-01 22:14:50	PE Event	PE	...b	127095	PE Type: Dynamic Link Library (DLL)
69		2022-03-01 22:14:51	PE Event	PE	...b	127097	PE Type: Dynamic Link Library (DLL)
70		2022-03-01 22:14:52	PE Event	PE	...b	127099	PE Type: Dynamic Link Library (DLL)
71		2022-03-01 22:14:53	PE Event	PE	...b	127101	PE Type: Dynamic Link Library (DLL)
72		2022-03-01 22:14:53	PE Event	PE	...b	127103	PE Type: Dynamic Link Library (DLL)
73		2022-03-01 22:14:54	PE Event	PE	...b	127105	PE Type: Dynamic Link Library (DLL)
74		2022-03-01 22:14:55	PE Event	PE	...b	127107	PE Type: Dynamic Link Library (DLL)
75		2022-03-01 22:14:56	PE Event	PE	...b	127109	PE Type: Dynamic Link Library (DLL)
76		2022-03-01 22:14:57	PE Event	PE	...b	127111	PE Type: Dynamic Link Library (DLL)
77		2022-03-01 22:14:58	PE Event	PE	...b	127113	PE Type: Dynamic Link Library (DLL)
78		2022-03-01 22:15:04	PE Event	PE	...b	127115	PE Type: Dynamic Link Library (DLL)
79		2022-03-01 22:15:18	PE Event	PE	...b	127117	PE Type: Dynamic Link Library (DLL)
80		2022-03-01 22:15:29	PE Event	PE	...b	127119	PE Type: Dynamic Link Library (DLL)
81		2022-03-01 22:15:37	PE Event	PE	...b	127121	PE Type: Dynamic Link Library (DLL)
82		2022-03-01 22:15:46	PE Event	PE	...b	127123	PE Type: Dynamic Link Library (DLL)
83		2022-03-01 22:15:57	PE Event	PE	...b	127125	PE Type: Dynamic Link Library (DLL)
84		2022-03-01 22:16:18	PE Event	PE	...b	127127	PE Type: Dynamic Link Library (DLL)
85		2022-03-01 22:30:02	PE Event	PE	...b	82809	PE Type: Executable (EXE) Import hash: c757b6532bf3304f2e1da07efe23042e
86		2022-03-01 22:30:02	PE Event	PE	...b	89341	PE Type: Executable (EXE) Import hash: c757b6532bf3304f2e1da07efe23042e
87		2022-03-05 03:19:27	PE Event	PE	...b	32865	PE Type: Executable (EXE) Import hash: 73effd46557538d5fa5561eee3ffc59c
88		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: fd490a0262febd37990bdbd445c01509
89		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: fd490a0262febd37990bdbd445c01509
90		2022-03-09 16:48:30	PE Event	PE	...b	54463	PE Type: Dynamic Link Library (DLL) Import hash: fd490a0262febd37990bdbd445c01509
91		2022-03-09 16:48:30	PE Event	PE	...b	54463	PE Type: Dynamic Link Library (DLL) Import hash: fd490a0262febd37990bdbd445c01509
92		2022-03-11 19:30:07	File stat	FILE	m..b	0	NTFS:\Users\IEUser\AppData\Local\Temp\wctFD02.tmp Type: file
93		2022-03-11 19:33:44	File stat	FILE	m..b	0	NTFS:\Users\IEUser\AppData\Local\Temp\wctF1F5.tmp Type: file
94		2022-03-14 18:18:04	PE Event	PE	...b	82876	PE Type: Dynamic Link Library (DLL)
95		2022-03-14 18:18:04	PE Event	PE	...b	82878	PE Type: Dynamic Link Library (DLL)
96		2022-03-14 18:53:38	File stat	FILE	ma.b	0	NTFS:\Users\IEUser\AppData\Local\Microsoft\Windows\Notifications\wpnidm\1c7f31e8.png Type: file
97		2022-03-14 19:14:17	PE Event	PE	...b	32881	PE Type: Executable (EXE) Import hash: 73effd46557538d5fa5561eee3ffc59c
98		2022-03-14 19:14:17	PE Event	PE	...b	32874	PE Type: Executable (EXE) Import hash: 73effd46557538d5fa5561eee3ffc59c
99		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		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		2022-03-15 16:56:35	PE Event	PE	...b	40112	PE Type: Dynamic Link Library (DLL) Import hash: 4a828507e62d541bc643dd70e74340c8

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
T	-	-	Values Text Filters
42	<input type="checkbox"/>	2022-03-01 22:14:22	PE Event
43	<input type="checkbox"/>	2022-03-01 22:14:23	PE Event
44	<input type="checkbox"/>	2022-03-01 22:14:24	PE Event
45	<input type="checkbox"/>	2022-03-01 22:14:25	PE Event
46	<input type="checkbox"/>	2022-03-01 22:14:26	PE Event
47	<input type="checkbox"/>	2022-03-01 22:14:27	PE Event
48	<input type="checkbox"/>	2022-03-01 22:14:28	PE Event
49	<input type="checkbox"/>	2022-03-01 22:14:29	PE Event
50	<input type="checkbox"/>	2022-03-01 22:14:30	PE Event
51	<input type="checkbox"/>	2022-03-01 22:14:30	PE Event
52	<input type="checkbox"/>	2022-03-01 22:14:31	PE Event
53	<input type="checkbox"/>	2022-03-01 22:14:32	PE Event
54	<input type="checkbox"/>	2022-03-01 22:14:35	PE Event
55	<input type="checkbox"/>	2022-03-01 22:14:36	PE Event
56	<input type="checkbox"/>	2022-03-01 22:14:38	PE Event
57	<input type="checkbox"/>	2022-03-01 22:14:39	PE Event
58	<input type="checkbox"/>	2022-03-01 22:14:40	PE Event
59	<input type="checkbox"/>	2022-03-01 22:14:41	PE Event
60	<input type="checkbox"/>	2022-03-01 22:14:42	PE Event
61	<input type="checkbox"/>	2022-03-01 22:14:43	PE Event
62	<input type="checkbox"/>	2022-03-01 22:14:44	PE Event
63	<input type="checkbox"/>	2022-03-01 22:14:45	PE Event
64	<input type="checkbox"/>	2022-03-01 22:14:46	PE Event
65	<input type="checkbox"/>	2022-03-01 22:14:47	PE Event
66	<input type="checkbox"/>	2022-03-01 22:14:48	PE Event
67	<input type="checkbox"/>	2022-03-01 22:14:49	PE Event
68	<input type="checkbox"/>	2022-03-01 22:14:50	PE Event
69	<input type="checkbox"/>	2022-03-01 22:14:51	PE Event
70	<input type="checkbox"/>	2022-03-01 22:14:52	PE Event
71	<input type="checkbox"/>	2022-03-01 22:14:53	PE Event
72	<input type="checkbox"/>	2022-03-01 22:14:53	PE Event
73	<input type="checkbox"/>	2022-03-01 22:14:54	PE Event
74	<input type="checkbox"/>	2022-03-01 22:14:55	PE Event
75	<input type="checkbox"/>	2022-03-01 22:14:56	PE Event
76	<input type="checkbox"/>	2022-03-01 22:14:57	PE Event
77	<input type="checkbox"/>	2022-03-01 22:14:58	PE Event
--	<input type="checkbox"/>	--	--

Enter text to search...

- (All)
- Amcache Registry Entry
- AppCompatCache Registry Entry
- BackgroundActivity Moderator Registry Entry
- File entry shell item
- File stat
- Mactime Bodyfile
- NTFS USN change
- OLECF Dest list entry
- OLECF Item
- PE Event
- Registry Key
- Registry Key - BagMRU
- Registry Key - Run Key
- Registry Key - Service
- Registry Key - Typed URLs
- Registry Key - User Account Information
- Registry Key - UserAssist
- Registry Key - Winlogon
- Registry Key Shutdown Entry
- System
- System - Network Connection
- Task Cache
- Windows Setupapi Log
- Windows Shortcut
- WinEVTX
- WinPrefetch

PE	...a	127107 PE Type: Dynamic Link Library (DLL)
PE	...b	127109 PE Type: Dynamic Link Library (DLL)
PE	...b	127111 PE Type: Dynamic Link Library (DLL)
PE	...b	127113 PE Type: Dynamic Link Library (DLL)

You can filter the specific events.

Activate Windows

Go to Settings to activate Windows



# Super timeline Analysis Malicious 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

ART-attack[ts1] art-attack.ps1

You can show all events

Line	Tag	Timestamp	Source Description	Source Name	macb	Inode	Long Description
128		2022-03-17 01:04:57	NTFS USN change	FILE	...	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
129		2022-03-17 01:04:57	NTFS USN change	FILE	...	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
130		2022-03-17 01:04:58	NTFS USN change	FILE	...	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
131		2022-03-17 01:04:58	NTFS USN change	FILE	...	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
132		2022-03-17 01:04:58	NTFS USN change	FILE	...	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
133		2022-03-17 01:04:58	NTFS USN change	FILE	...	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
134		2022-03-17 01:05:03	NTFS USN change	FILE	...	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
135		2022-03-17 01:05:03	NTFS USN change	FILE	...	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
136		2022-03-17 01:05:03	NTFS USN change	FILE	...	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
137		2022-03-17 01:05:03	NTFS USN change	FILE	...	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
138		2022-03-17 01:05:03	NTFS USN change	FILE	...	57177	EtwRTUBPM.etl File reference: 3495-4 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_FILE_CREATE
139		2022-03-17 01:05:03	NTFS USN change	FILE	...	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		2022-03-17 01:05:03	NTFS USN change	FILE	...	57177	EtwRTDiaglog.etl File reference: 80516-3 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
141		2022-03-17 01:05:03	NTFS USN change	FILE	...	57177	EtwRTDiaglog.etl File reference: 80516-3 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_DAT
142		2022-03-17 01:05:03	NTFS USN change	FILE	...	57177	EtwREventLog-System.etl File reference: 80517-3 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
143		2022-03-17 01:05:03	NTFS USN change	FILE	...	57177	EtwREventLog-System.etl File reference: 80517-3 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN RE
144		2022-03-17 01:05:03	NTFS USN change	FILE	...	57177	BCD.LOG File reference: 80504-3 Parent file reference: 80374-3 Update source: Update reason: USN_REASON_DATA_OVERWRITE
145		2022-03-17 01:05:04	NTFS USN change	FILE	...	57177	BCD File reference: 80503-3 Parent file reference: 80374-3 Update source: Update reason: USN_REASON_DATA_OVERWRITE
146		2022-03-17 01:05:04	NTFS USN change	FILE	...	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		2022-03-17 01:05:04	NTFS USN change	FILE	...	57177	EtwRTDiaglog.etl File reference: 80516-3 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_DAT
148		2022-03-17 01:05:04	NTFS USN change	FILE	...	57177	EtwREventLog-System.etl File reference: 80517-3 Parent file reference: 4312-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN RE
149		2022-03-17 01:05:04	NTFS USN change	FILE	...	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE
150		2022-03-17 01:05:04	NTFS USN change	FILE	...	57177	bootstat.dat File reference: 81810-1 Parent file reference: 1803-1 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
151		2022-03-17 01:05:04	NTFS USN change	FILE	...	57177	BCD File reference: 80503-3 Parent file reference: 80374-3 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
152		2022-03-17 01:05:04	NTFS USN change	FILE	...	57177	BCD.LOG File reference: 80504-3 Parent file reference: 80374-3 Update source: Update reason: USN_REASON_DATA_OVERWRITE USN_REASON_CLOSE
153		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		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		2022-03-17 15:26:04	PE Event	PE	...b	41640	PE Type: Dynamic Link Library (DLL) Import hash: 5d628e9abd82a65cfa9cdf396f6eb2aa
156		2022-03-17 15:26:04	PE Event	PE	...b	41640	PE Type: Dynamic Link Library (DLL) Import hash: 5d628e9abd82a65cfa9cdf396f6eb2aa
157		2022-03-17 16:10:41	PE Event	PE	...b	82877	PE Type: Dynamic Link Library (DLL)
158		2022-03-17 16:10:41	PE Event	PE	...b	82879	PE Type: Dynamic Link Library (DLL)
159		2022-03-17 16:17:09	PE Event	PE	...b	127811	PE Type: Dynamic Link Library (DLL)
160		2022-03-17 16:17:40	PE Event	PE	...b	127822	PE Type: Dynamic Link Library (DLL)
161		2022-03-17 16:27:16	AppCompatCache Regi...	REG	....	42071	[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\AppDataCache] Cached entry: 7 Path: C:\AtomicRedTeam\atomics\T1543.003\bin\A
162		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 Activate Windows

Timestamp Is same day 2022-03-17 00:00:00 2022-03-18 00:00:00 Go to Settings to activate Windows

C:\Cases\Analysis\Timeline\super-timeline.csv Total lines 119,983 Visible lines 98,243 Open files: 1 Search options

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

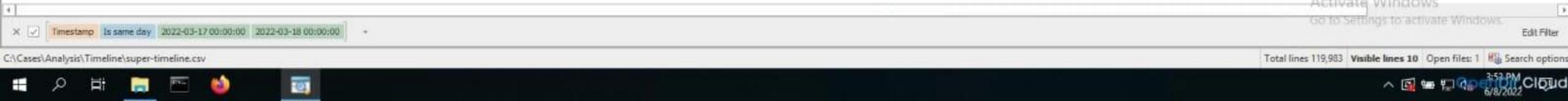
super-timeline.csv

Drag a column header here to group by that column

ART-attack.ps1

Line	Tag	Timestamp	Source Description	Source Name	macb	Inode	Long Description
T	-	-	-	-	-	-	-
920		2022-03-17 23:35:52	File stat	FILE	m..b	0	NTFS:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam\ART-attack.ps1 Type: file
32926		2022-03-18 00:17:31	NTFS USN change	FILE	...c.	57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE
32927		2022-03-18 00:17:31	NTFS USN change	FILE	...c.	57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE USN_REASON_CLO
32928		2022-03-18 00:17:31	NTFS USN change	FILE	...c.	57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASON_FILE_CREATE
32929		2022-03-18 00:17:31	NTFS USN change	FILE	...c.	57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_FILE_CREA
32930		2022-03-18 00:17:31	NTFS USN change	FILE	...c.	57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_FILE_CREA
32931		2022-03-18 00:17:31	NTFS USN change	FILE	...c.	57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE
32932		2022-03-18 00:17:31	NTFS USN change	FILE	...c.	57177	ART-attack.ps1 File reference: 84925-4 Parent file reference: 84923-4 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE USN_REASON_CLO
32933		2022-03-18 00:17:31	File stat	FILE	...c.	0	NTFS:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam\ART-attack.ps1 Type: file
43962		2022-03-18 00:20:49	File stat	FILE	.a..	0	NTFS:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam\ART-attack.ps1 Type: file

You can search specific events and show result.



super-timelapse.com

Drag a column header here to group by that column

atomicservice.exe

Using colorcode you know about execution on events.

Drag a column header here to group by that column

notepad.exe

Show all events in long  
description also.

Offset 140718688829440  
ize 69632 Offset 140718863417344  
Offset 140718872854528  
t 140718929543168  
set 140695128834048  
140718930395136  
set 140718847295488  
t 140718415282176  
ffset 140718863745024  
set 140718863548416  
set 140718923317248  
t 140718883340288  
Size 2150400 Offset 140718838251520  
Offset 140718866956288  
et 140718691647488  
set 140718834384896  
t 140718874230784  
Size 7643136 Offset 140718874689536  
Offset 140718801420288

-0A02-000000001200}' '6552' 'C:\Windows\system32\kernel32.dll'  
me: 1 [serial number: 0xB4A6FFC6 devic...  
set 140718862237696  
et 140718770028544  
55.001.dll) Size 118784 Offset 1407187...  
\_REASON\_DATA\_TRUNCATION  
\_REASON\_DATA\_EXTEND USN\_REASON\_DATA\_T...  
\_REASON\_DATA\_EXTEND USN\_REASON\_DATA\_T...  
Interval: [REG\_DWORD\_LE] 20160 ETag: [RE...  
rd  
d.exe Type: file

# 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