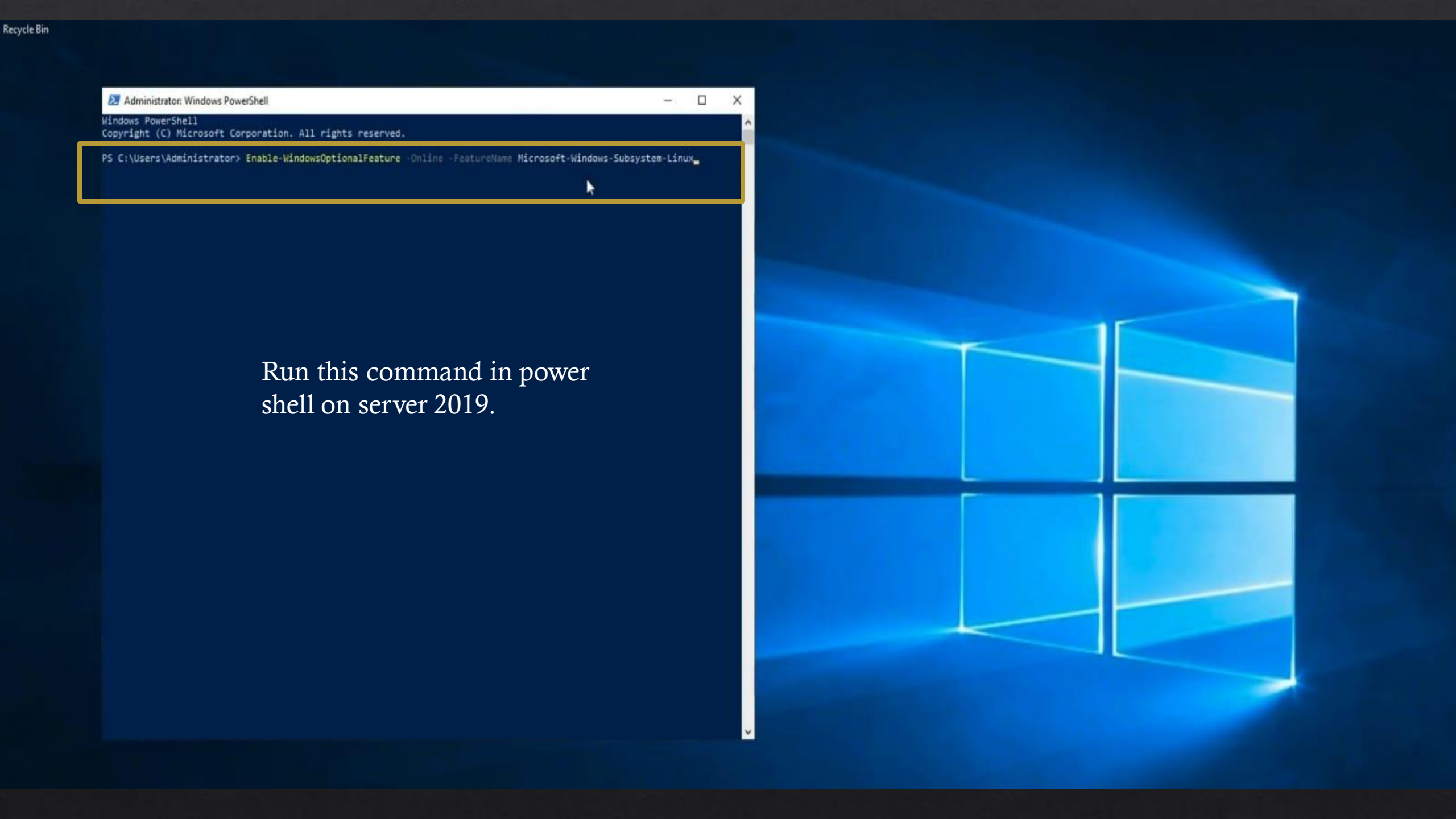
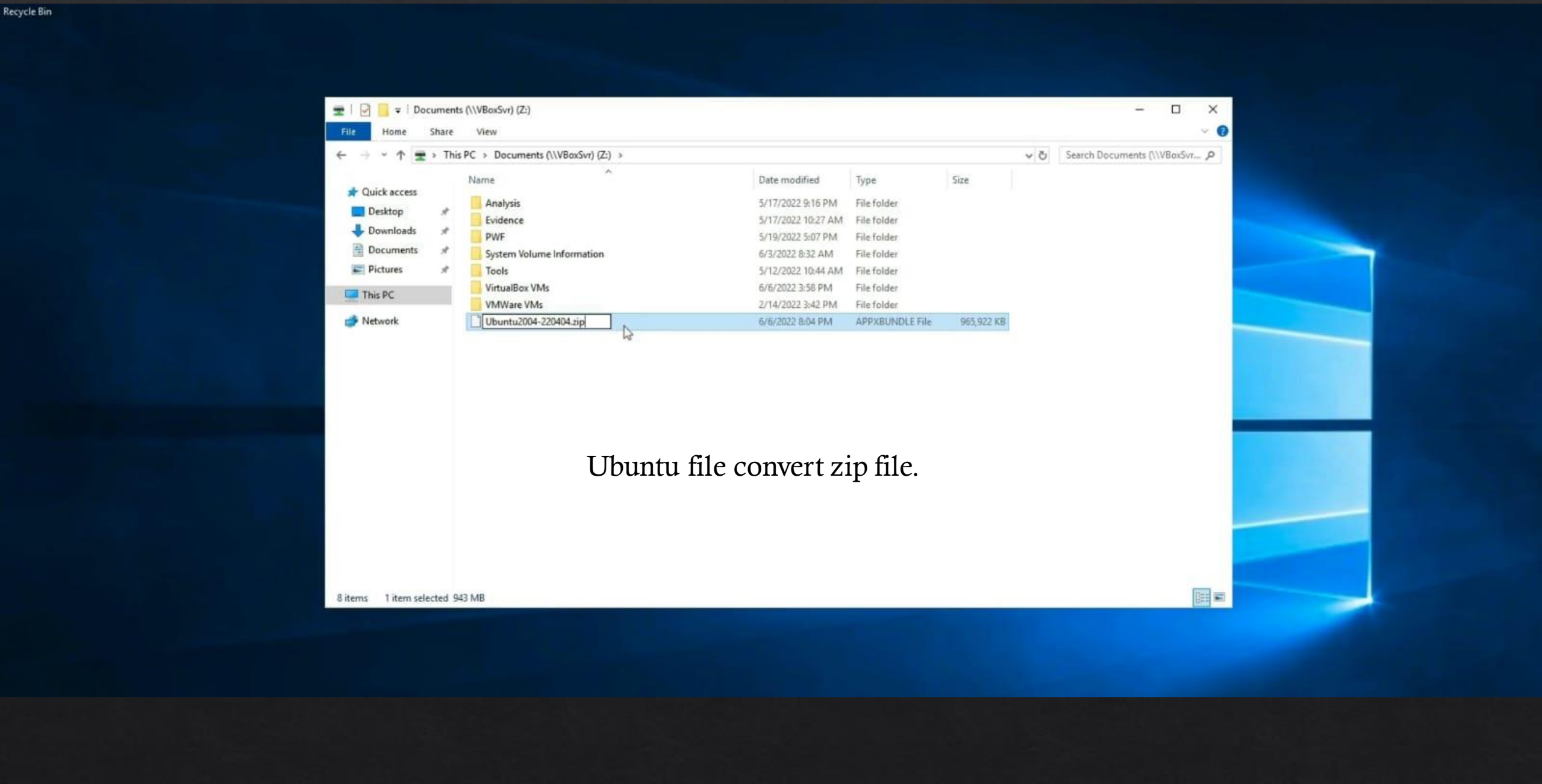
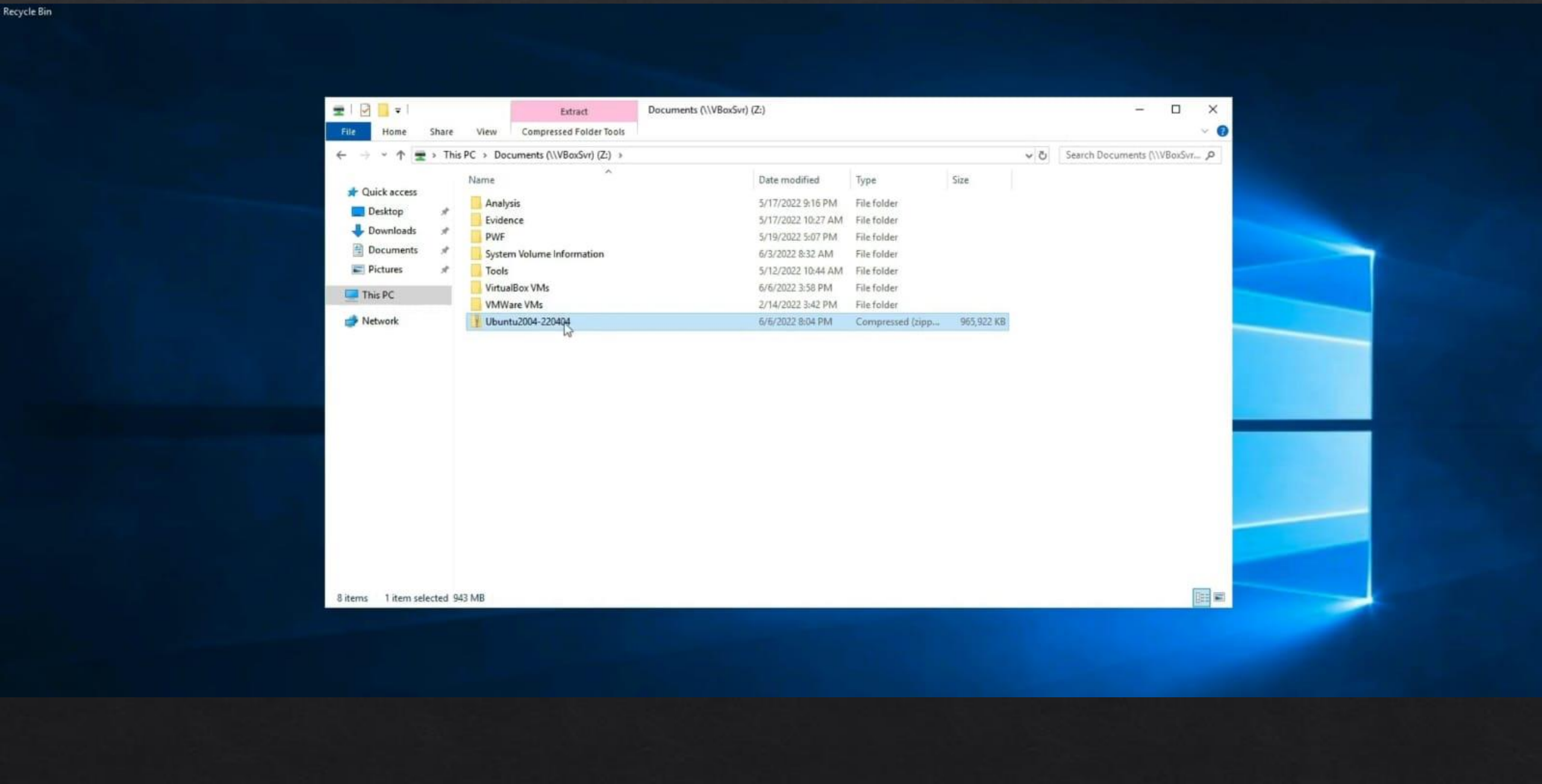
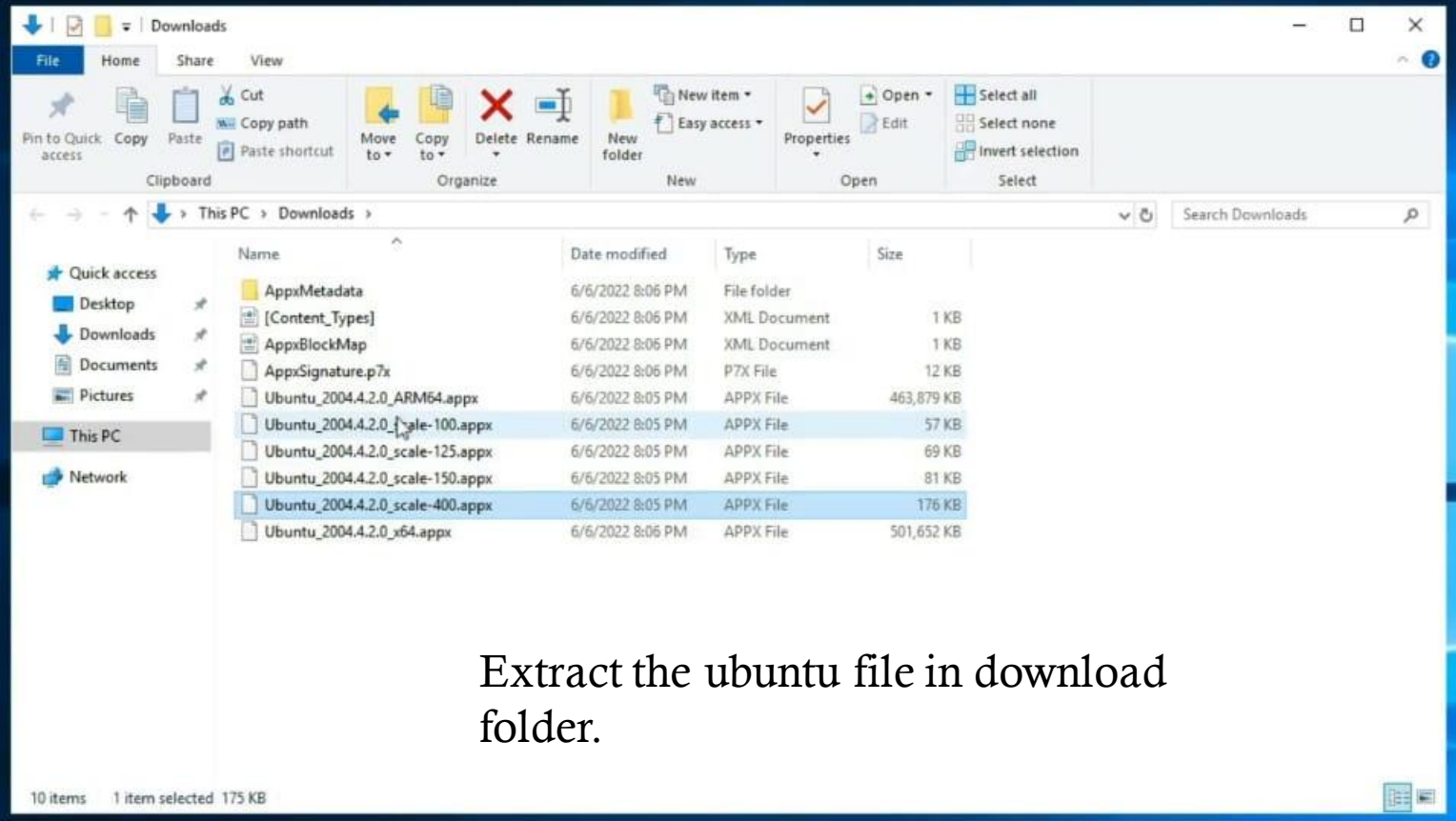
Windows Forensic


Recycle Bin
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.

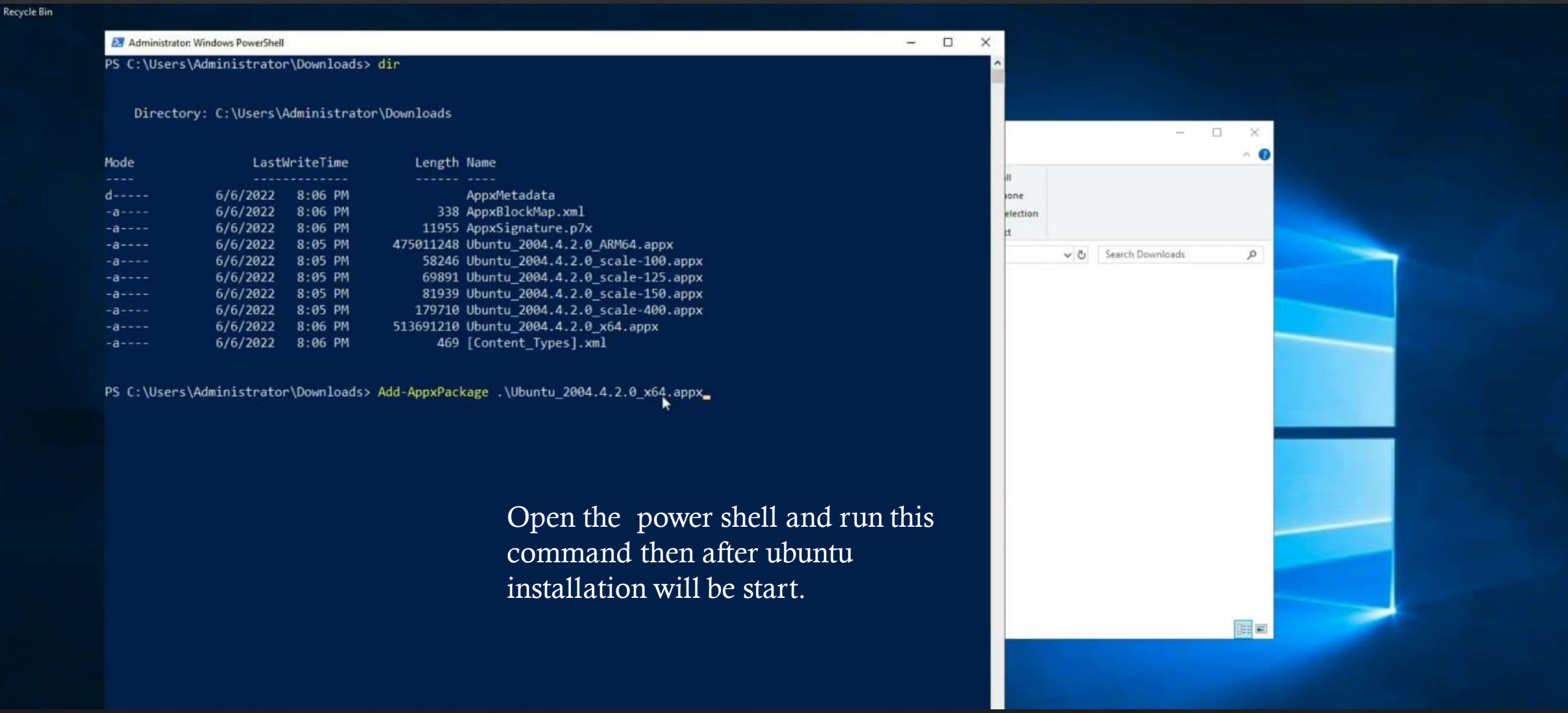


Ubuntu file convert zip file.

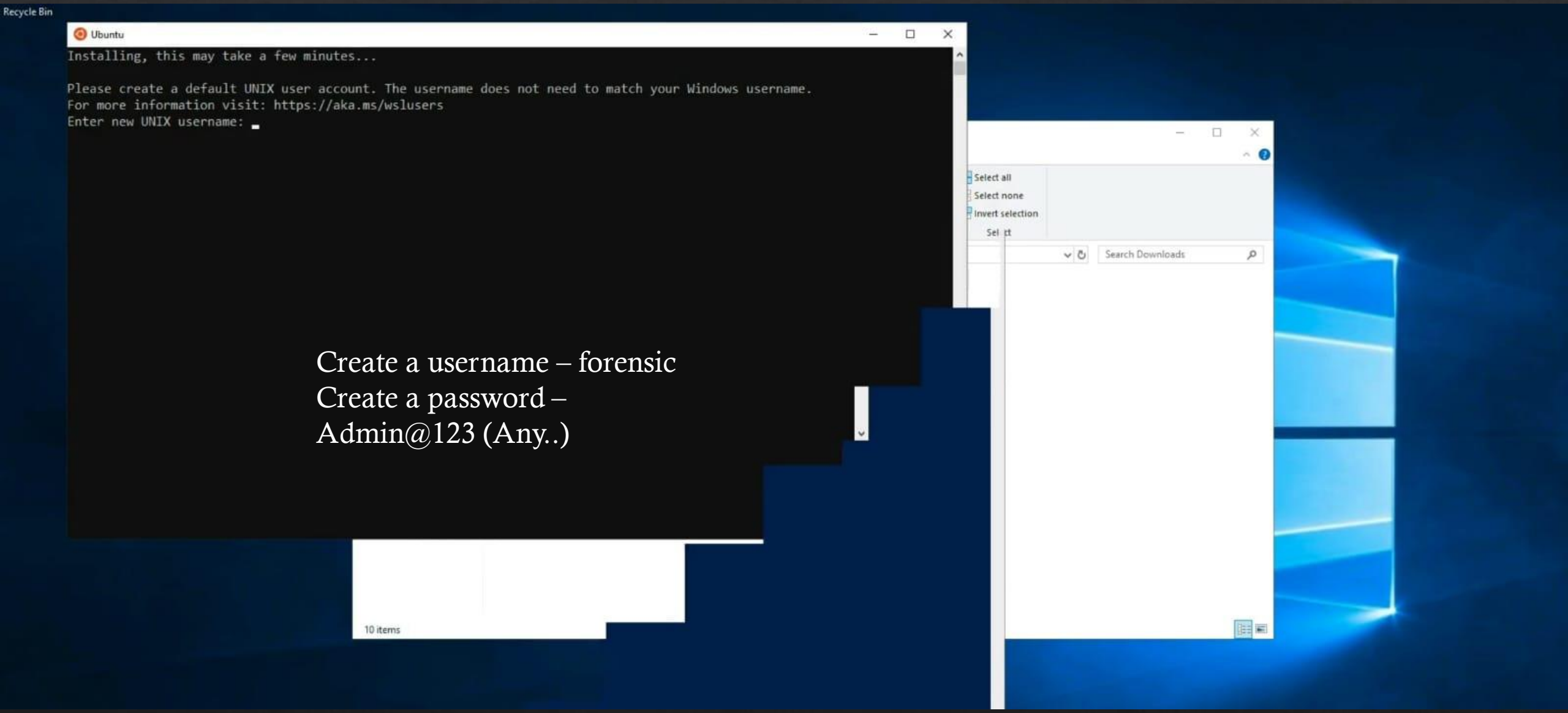

Recycle Bin
Extract
Documents (\\VBoxSvr) (Z:)
File
Home
Share
View
Compressed Folder Tools
This PC › Documents (\\VBoxSvr) (Z:) ›
Search Documents (\\VBoxSvr...
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
Analysis 5/17/2022 9:16 PM File folder
Evidence 5/17/2022 10:27 AM File folder
PWF 5/19/2022 5:07 PM File folder
System Volume Information 6/3/2022 8:32 AM File folder
Tools 5/12/2022 10:44 AM File folder
VirtualBox VMs 6/6/2022 3:58 PM File folder
VMWare VMs 2/14/2022 3:42 PM File folder
Ubuntu2004-220404 6/6/2022 8:04 PM Compressed (zipp... 965,922 KB
8 items
1 item selected 943 MB



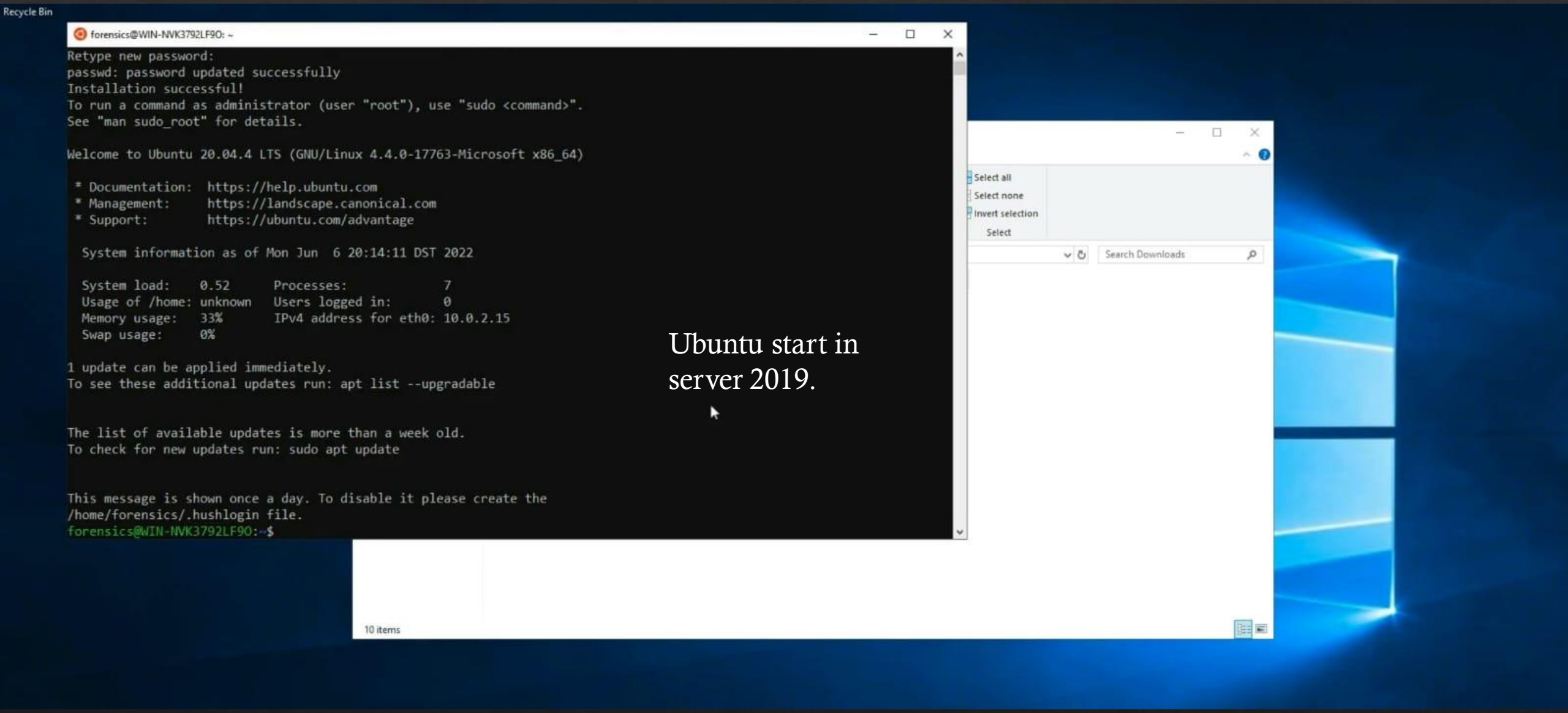
Extract the ubuntu file in download folder.

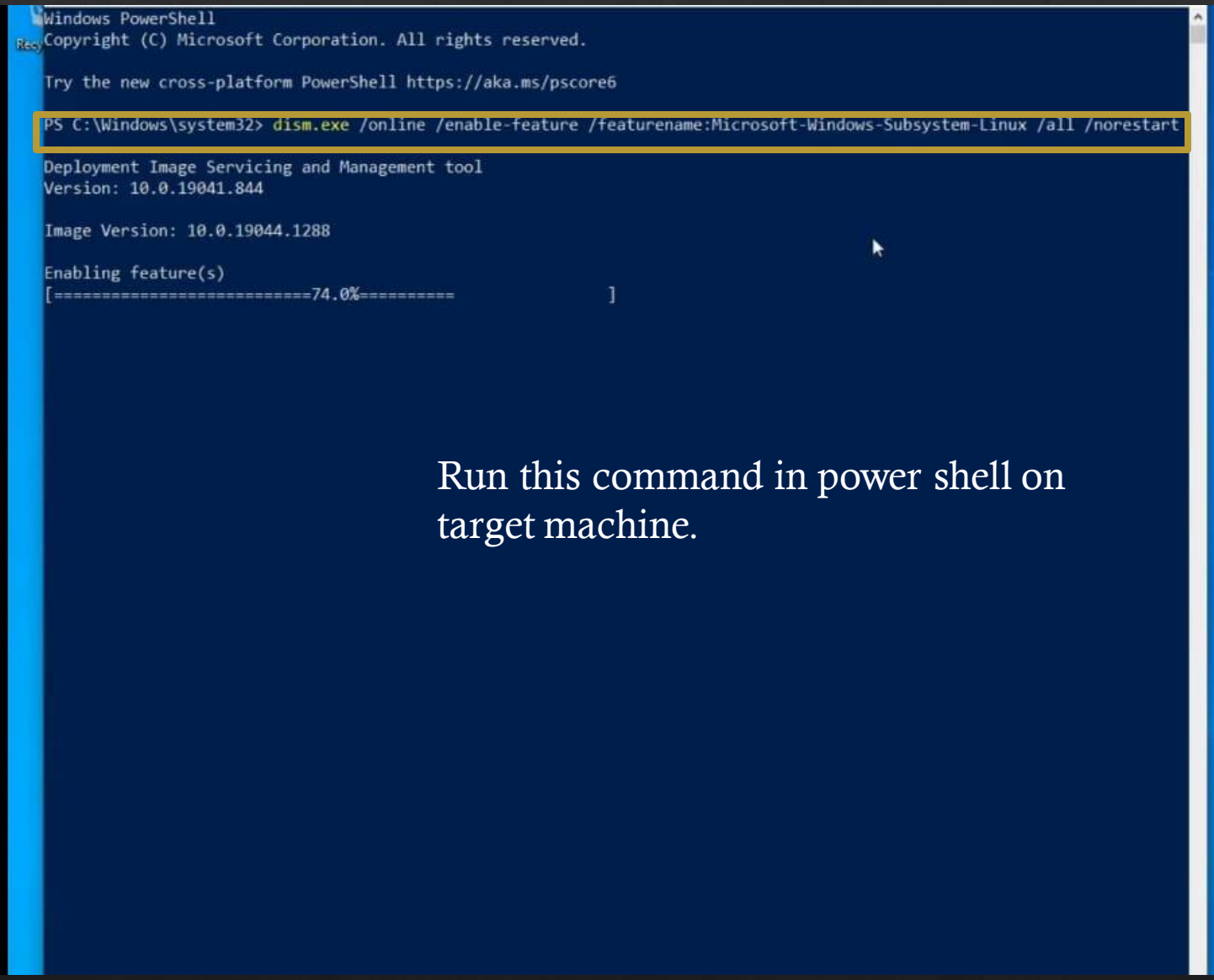


Open the power shell and run this command then after ubuntu installation will be start.

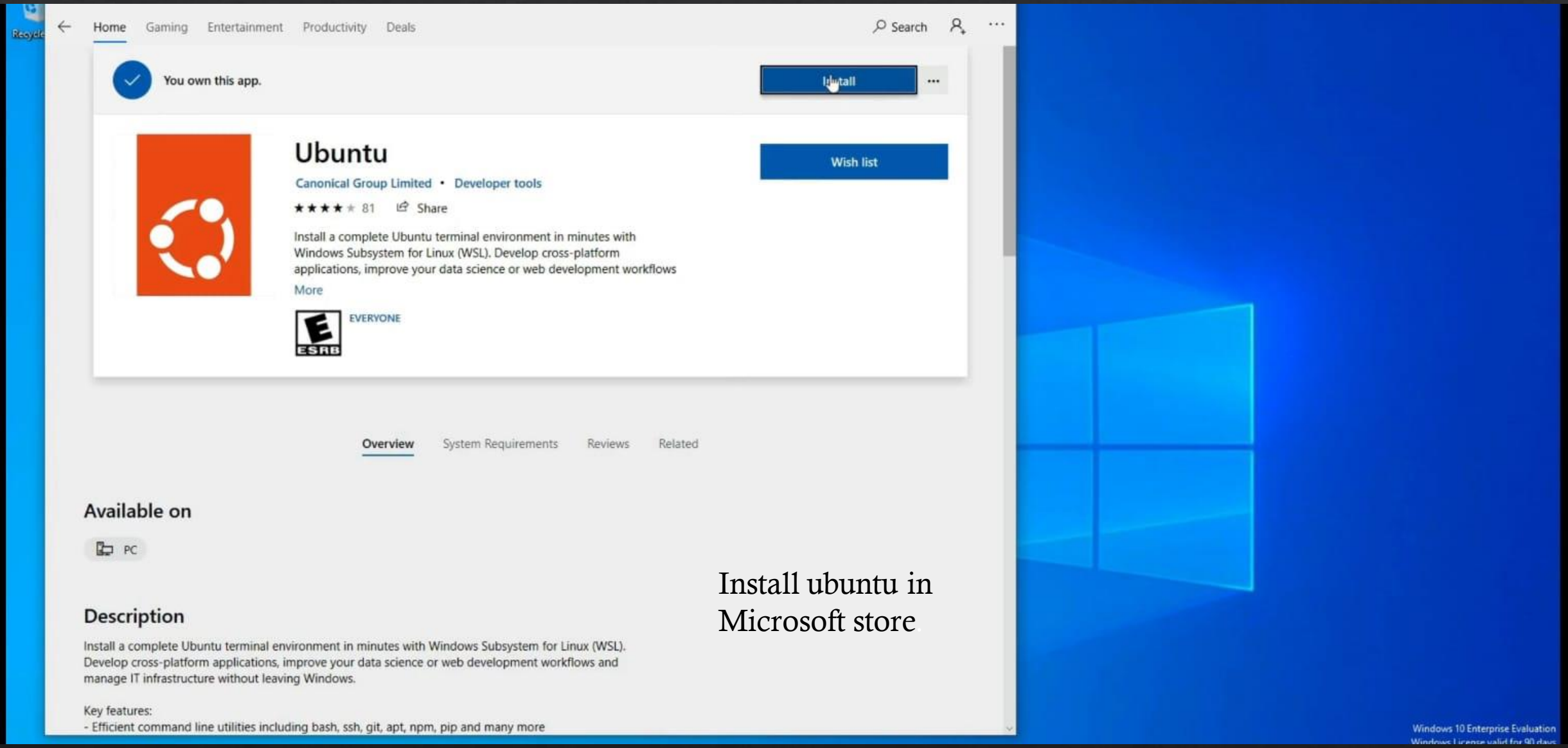


Create a username – forensic
Create a password –
Admin@123 (Any..)

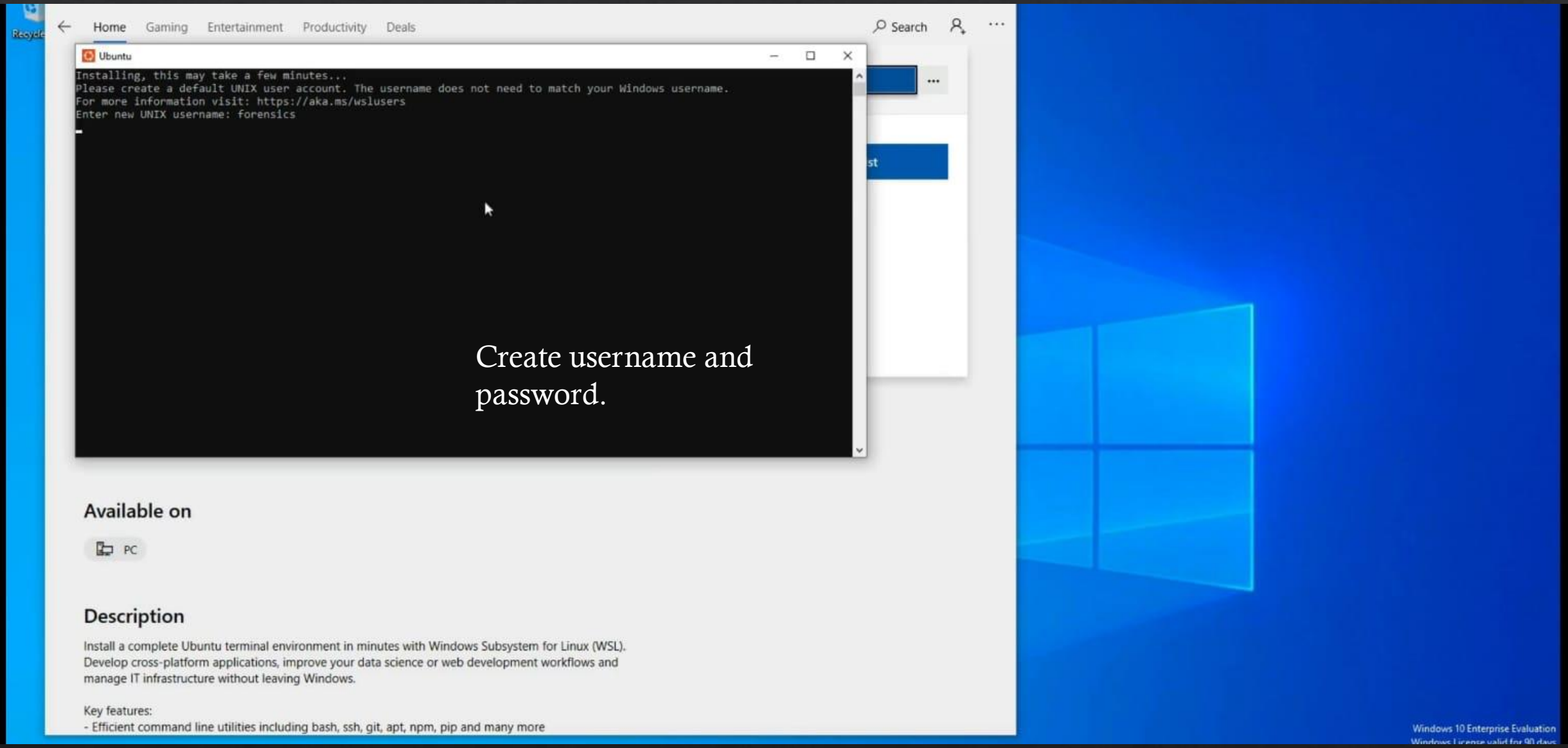

Recycle Bin
forensics@WIN-NVK3792LF9O: ~
Retype new password:
passwd: password updated successfully
Installation successful!
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 4.4.0-17763-Microsoft x86_64)
* 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-NVK3792LF9O:~$
Ubuntu start in server 2019.
Select all
Select none
Invert selection
Select
Search Downloads
10 items



Run this command in power shell on target machine.



Install ubuntu in Microsoft store


Home
Gaming
Entertainment
Productivity
Deals
Search
Ubuntu
Installing, this may take a few minutes...
Please create a default UNIX user account. The username does not need to match your Windows username.
For more information visit: https://aka.ms/wslusers
Enter new UNIX username: forensics
Create username and password.
Available on
PC
Description
Install a complete Ubuntu terminal environment in minutes with Windows Subsystem for Linux (WSL).
Develop cross-platform applications, improve your data science or web development workflows and
manage IT infrastructure without leaving Windows.
Key features:
- Efficient command line utilities including bash, ssh, git, apt, npm, pip and many more
Windows 10 Enterprise Evaluation

6. Open server 2019 and chage 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 > Exclution – Add click and select cases and tools folder one by one. And create a snapshort.

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

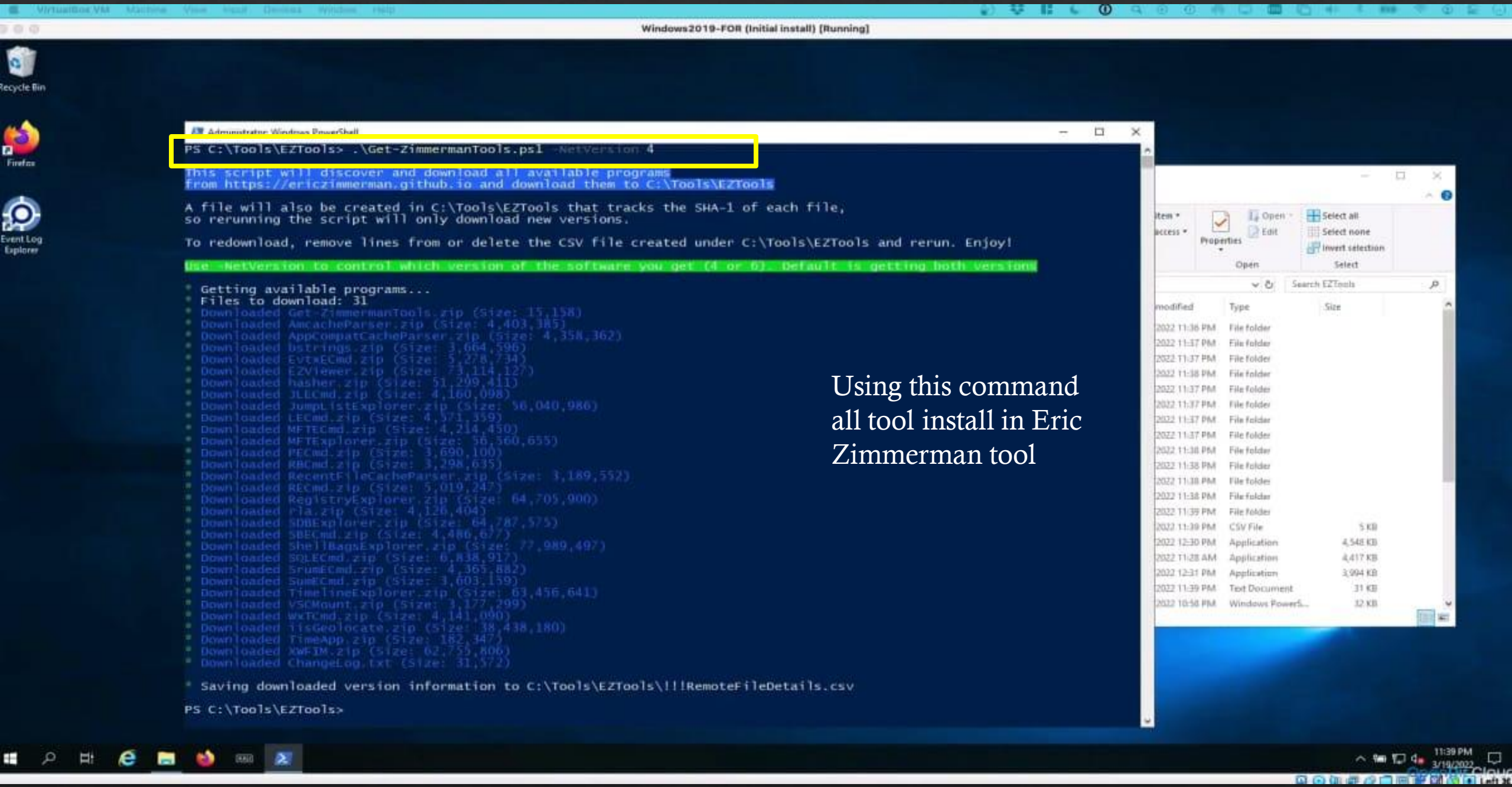
5. Download the event log explorer – https://eventlogxp.com/

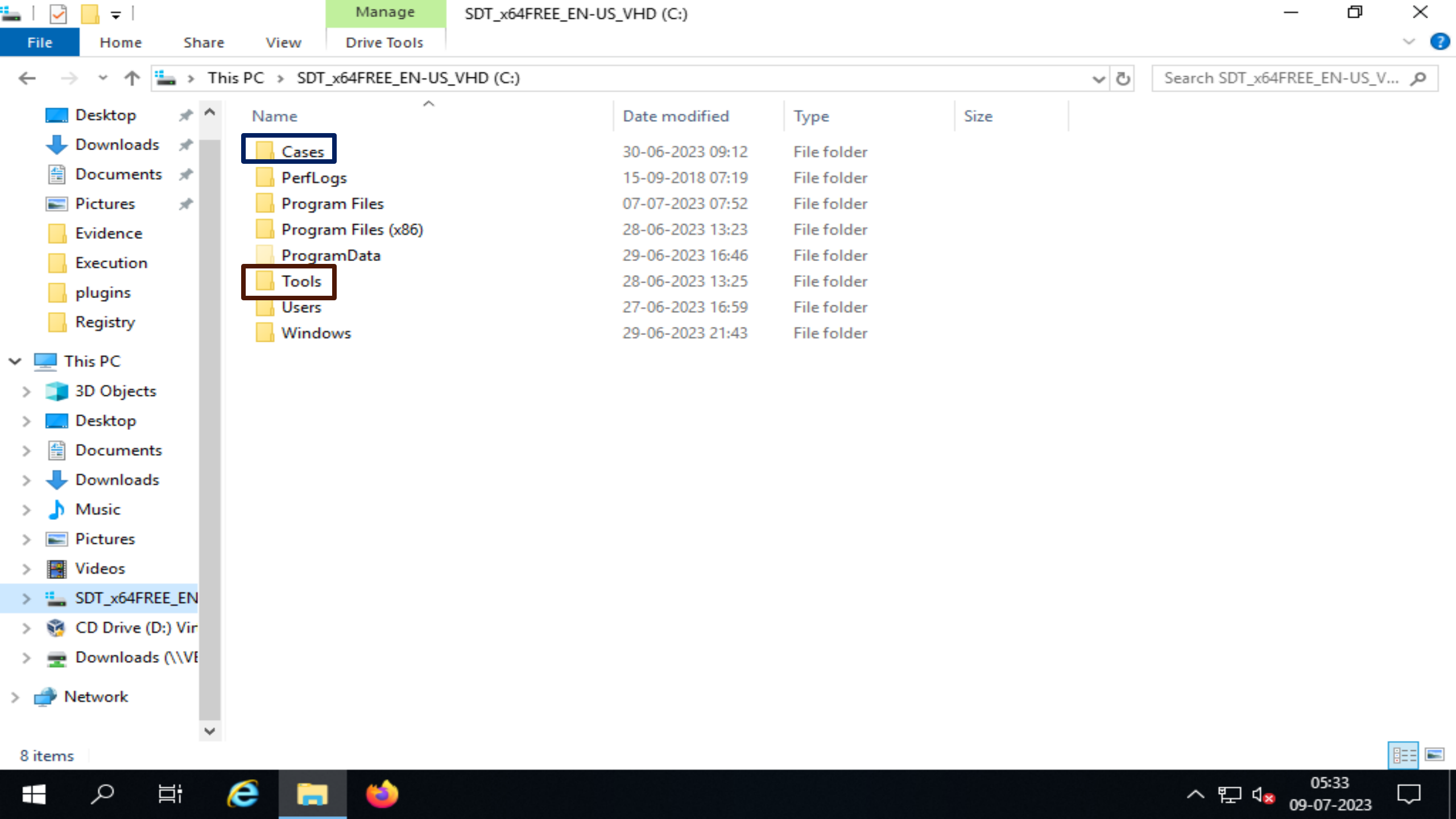
6. Download Notepad++ - https://notepad-plus-plus.org/downloads/

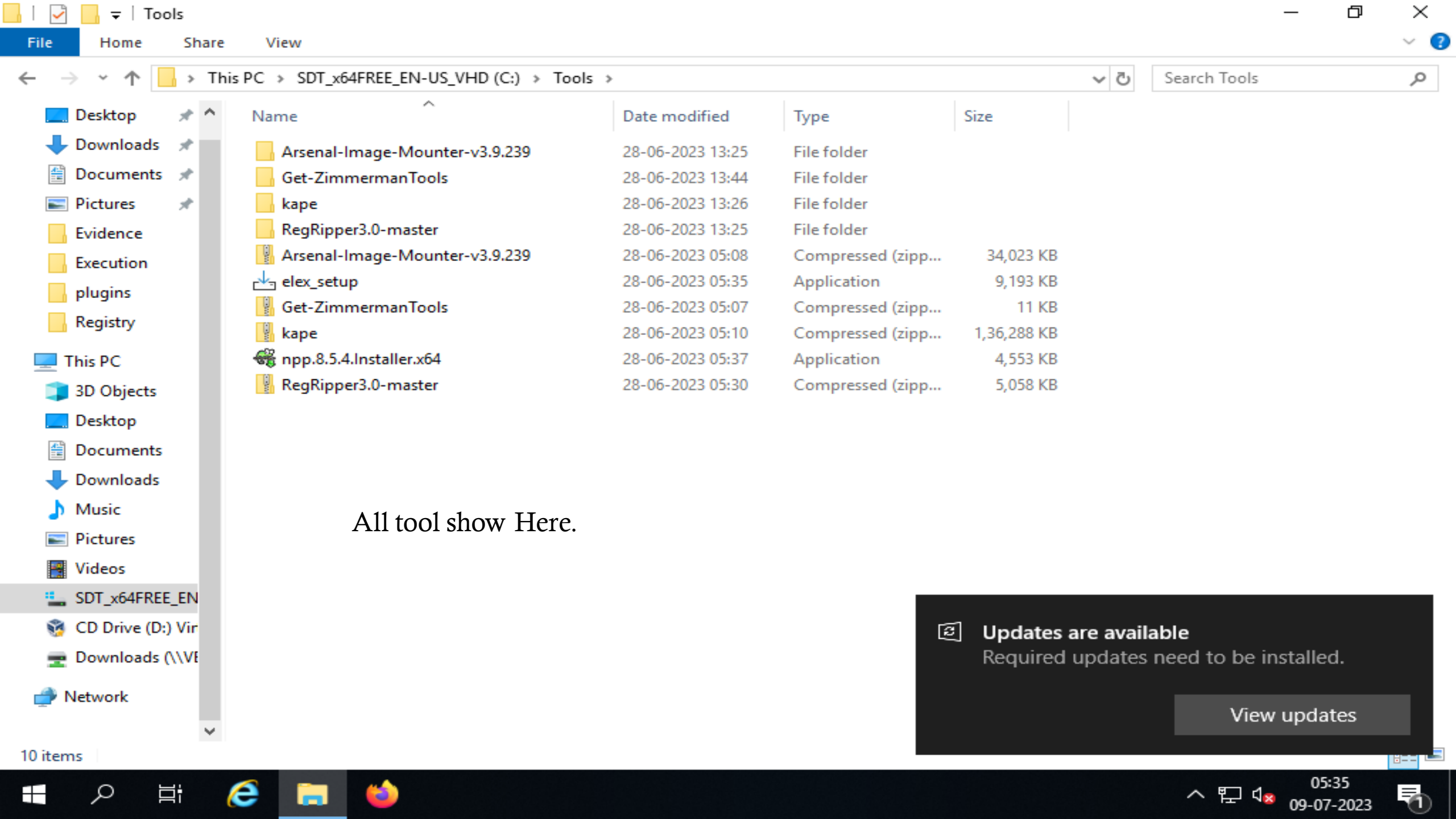
All tool copy in c drive Tools folder.

Installl the setup of Event log and Notepad++.

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


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 AmcacheParser.zip (Size: 4,403,385)
* Downloaded AppCompatCacheParser.zip (Size: 4,358,362)
* Downloaded bstrings.zip (Size: 3,664,596)
* Downloaded EvtxECmd.zip (Size: 5,278,734)
* Downloaded EZViewer.zip (Size: 73,114,127)
* Downloaded hasher.zip (Size: 51,299,411)
* Downloaded JLECmd.zip (Size: 4,160,098)
* Downloaded JumpListExplorer.zip (Size: 56,040,986)
* Downloaded LECmd.zip (Size: 4,571,359)
* Downloaded MFTECmd.zip (Size: 4,214,450)
* Downloaded MFTExplorer.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 RECmd.zip (Size: 5,019,247)
* Downloaded RegistryExplorer.zip (Size: 64,705,900)
* Downloaded rla.zip (Size: 4,126,404)
* Downloaded SDBExplorer.zip (Size: 64,787,575)
* Downloaded SBECmd.zip (Size: 4,486,677)
* Downloaded ShellBagsExplorer.zip (Size: 77,989,497)
* Downloaded SQLECmd.zip (Size: 6,838,917)
* Downloaded SrumECmd.zip (Size: 4,365,882)
* Downloaded SumECmd.zip (Size: 3,603,159)
* Downloaded TimelineExplorer.zip (Size: 63,456,641)
* Downloaded VSCMount.zip (Size: 3,177,299)
* Downloaded WxTCmd.zip (Size: 4,141,000)
* Downloaded iisGeolocate.zip (Size: 38,438,180)
* Downloaded TimeApp.zip (Size: 182,347)
* Downloaded XWFIM.zip (Size: 62,755,806)
* Downloaded ChangeLog.txt (Size: 31,572)
* Saving downloaded version information to C:\Tools\EZTools\!!!RemoteFileDetails.csv
PS C:\Tools\EZTools>
Using this command all tool install in Eric Zimmerman tool
Properties
Open
Edit
Select all
Select none
Invert selection
Select
Search EZTools
Modified
Type
Size
File folder
CSV File
Application
Text Document
Windows PowerS...
11:39 PM
3/19/2022


Manage
SDT_x64FREE_EN-US_VHD (C:)
File
Home
Share
View
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 (\\VE
Network
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
8 items
05:33
09-07-2023


Tools
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 (\\VE
Network
Name
Date modified
Type
Size
Arsenal-Image-Mounter-v3.9.239 28-06-2023 13:25 File folder
Get-ZimmermanTools 28-06-2023 13:44 File folder
kape 28-06-2023 13:26 File folder
RegRipper3.0-master 28-06-2023 13:25 File folder
Arsenal-Image-Mounter-v3.9.239 28-06-2023 05:08 Compressed (zipp... 34,023 KB
elex_setup 28-06-2023 05:35 Application 9,193 KB
Get-ZimmermanTools 28-06-2023 05:07 Compressed (zipp... 11 KB
kape 28-06-2023 05:10 Compressed (zipp... 1,36,288 KB
npp.8.5.4.Installer.x64 28-06-2023 05:37 Application 4,553 KB
RegRipper3.0-master 28-06-2023 05:30 Compressed (zipp... 5,058 KB
All tool show Here.
Updates are available
Required updates need to be installed.
View updates
10 items
05:35
09-07-2023

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

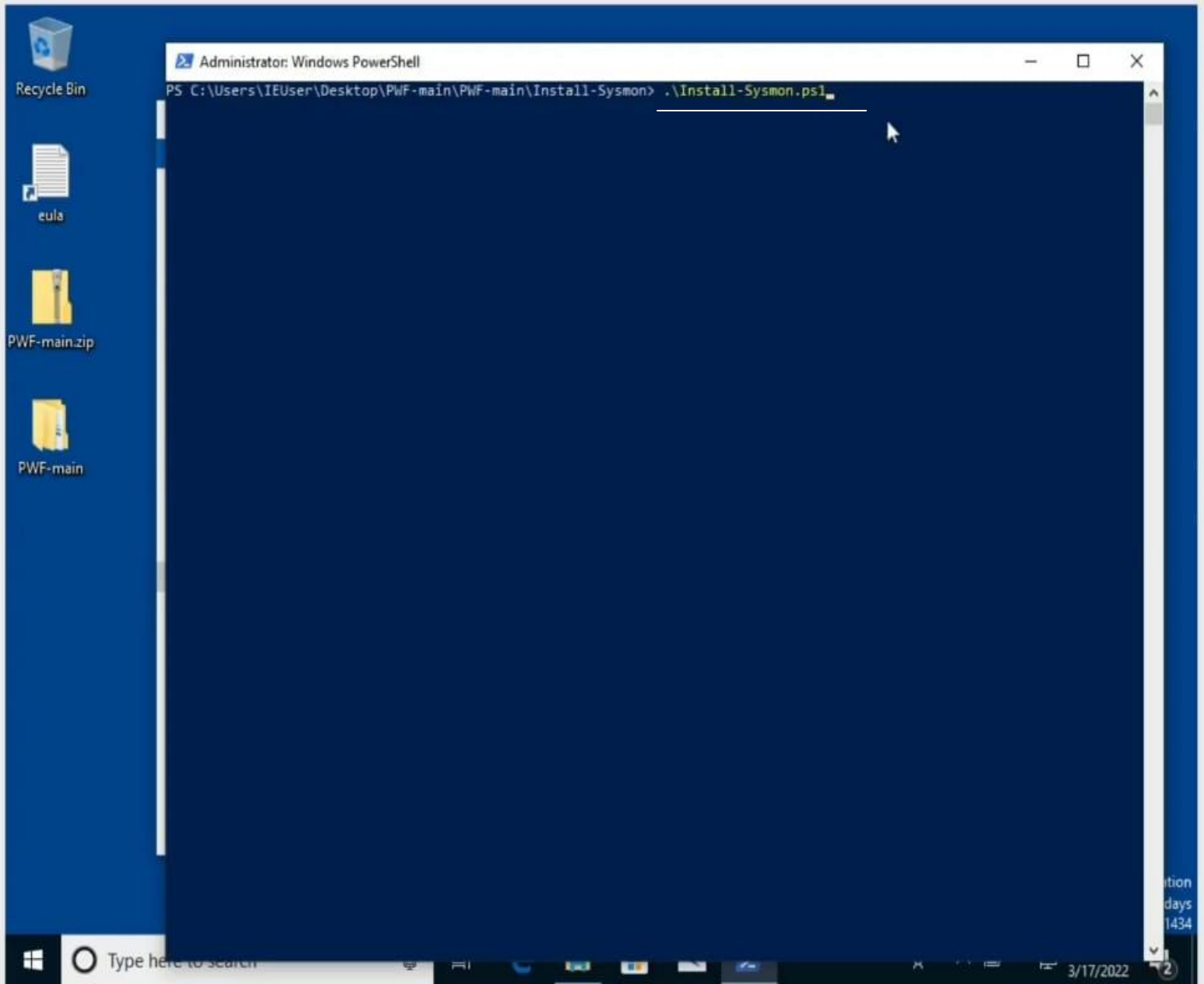
zip file download and extract file.

2 script is execute here.

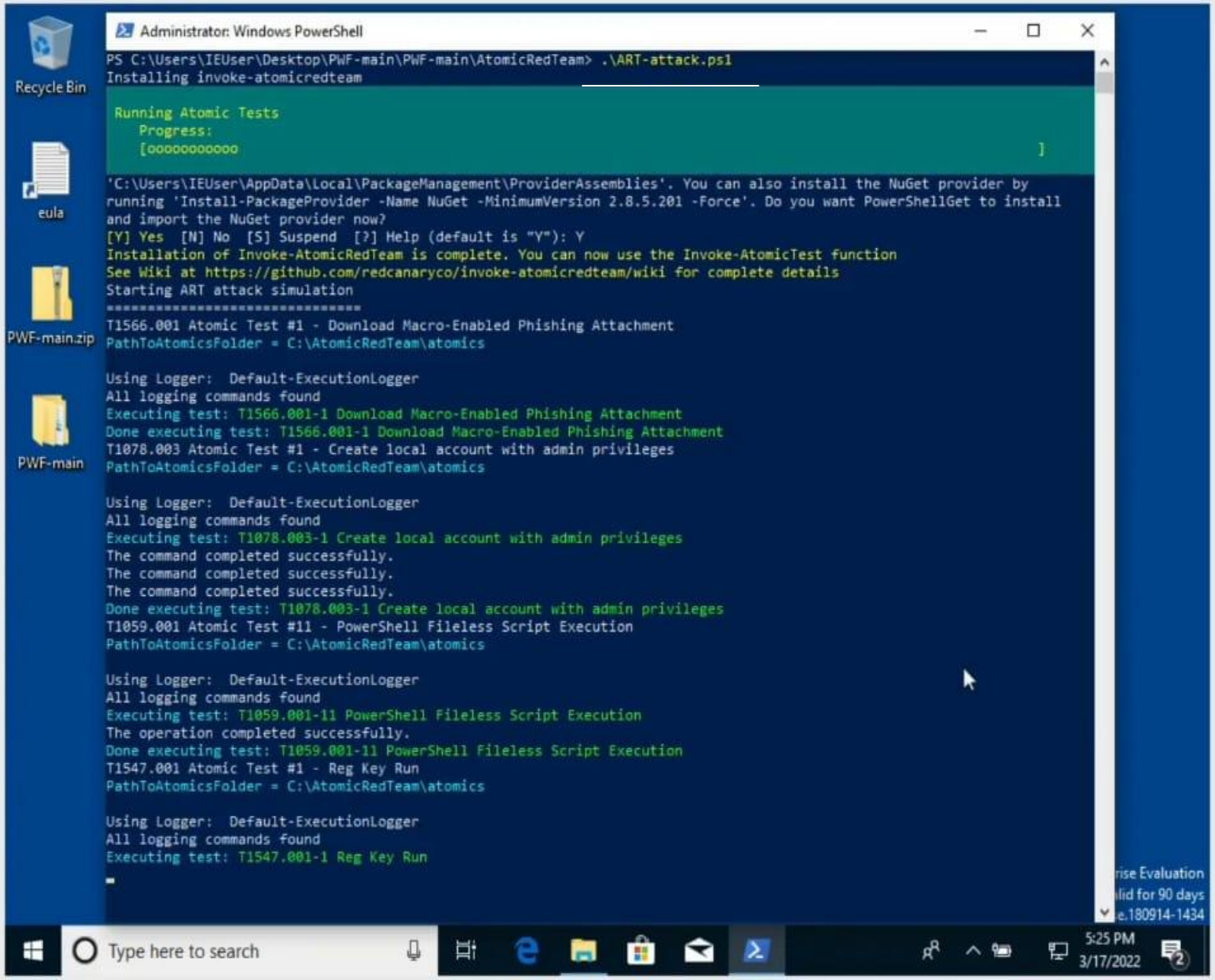
1. Sysmon script – C:\users\denisha\Desktop\PWF-main\PWF-main/Install-Sysmon > powershell as administrator > .\Install-sysmon.ps1.

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

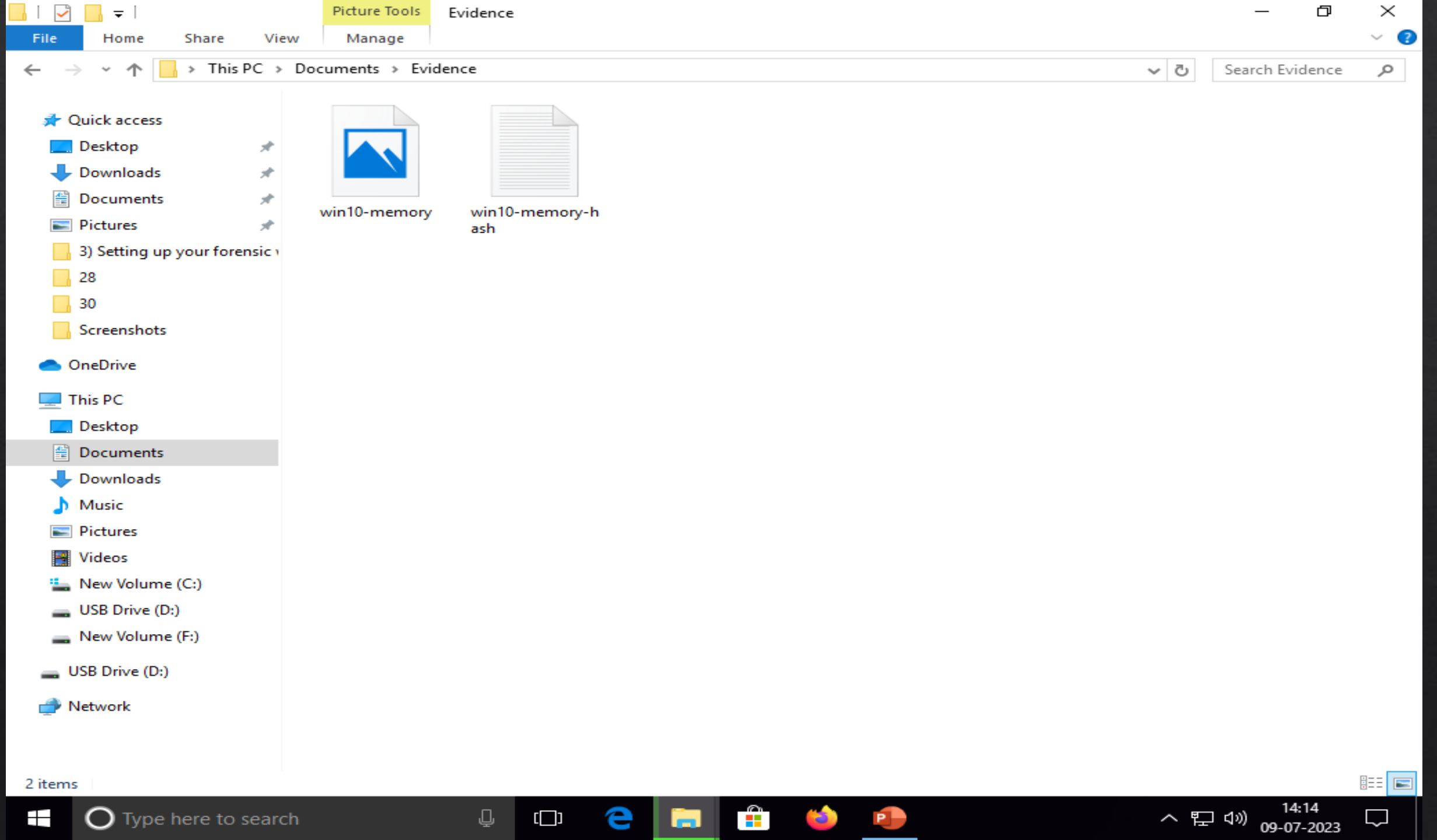


Data Collection

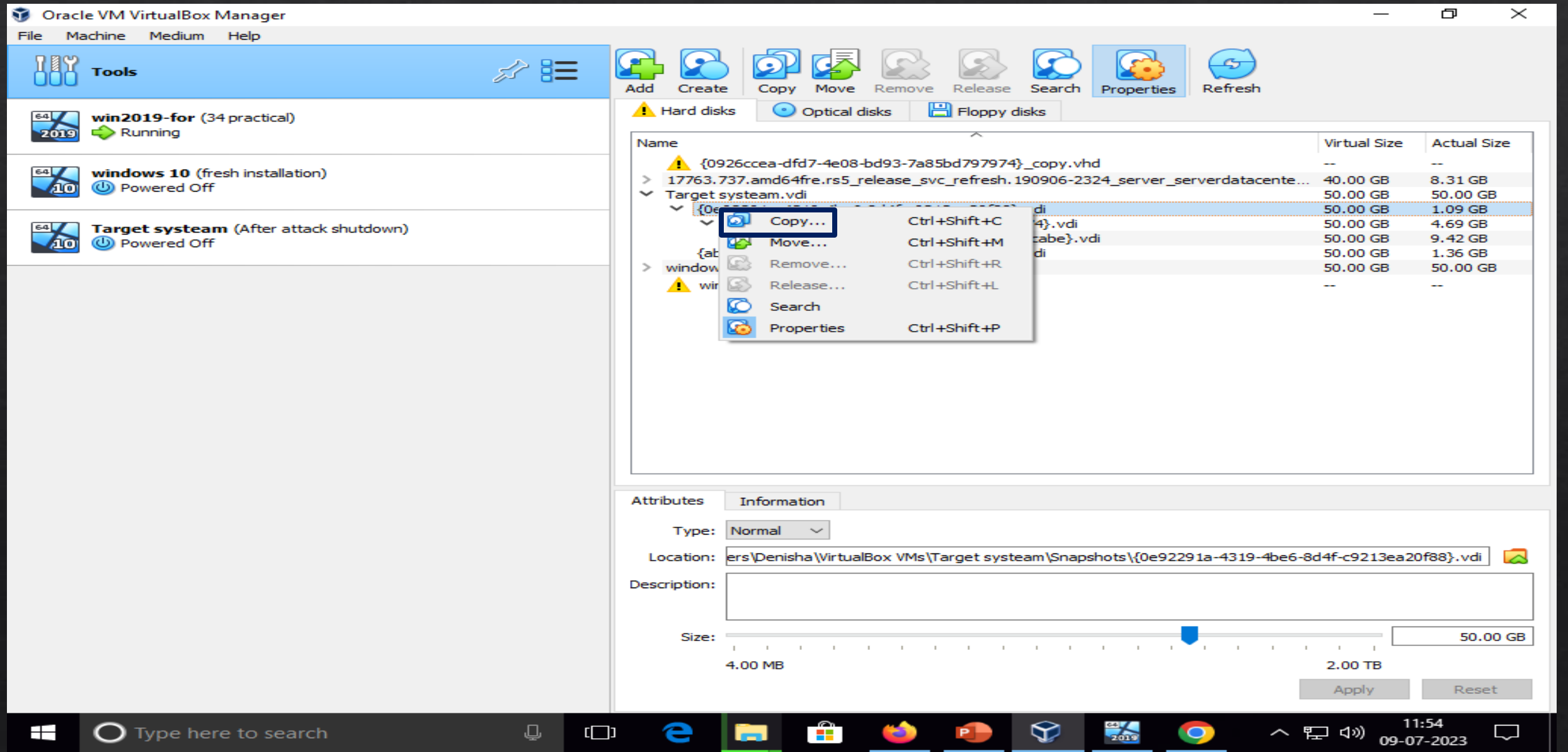
9.Memory Acquisition of the target system

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.


Picture Tools
Evidence
File
Home
Share
View
Manage
This PC
Documents
Evidence
Search Evidence
Quick access
Desktop
Downloads
Documents
Pictures
3) Setting up your forensic
28
30
Screenshots
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
New Volume (C:)
USB Drive (D:)
New Volume (F:)
USB Drive (D:)
Network
win10-memory
win10-memory-hash
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 systeam (After attack
Powered Off

Add Create Copy Move Remove Release Search Properties Refresh

Hard disks Optical disks Floppy disks

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

Copy Virtual Disk

Virtual Hard disk file type

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

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

Expert Mode Back Next Cancel

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

Description:

Size: 50.00 GB

4.00 MB 2.00 TB

Apply Reset

Type here to search

11:54
09-07-2023

Oracle VM VirtualBox Manager

File Machine Medium Help

Tools

win2019-for (34 practical)
Running

windows 10 (fresh installation)
Powered Off

Target systeam (After attack
Powered Off

Add Create Copy Move Remove Release Search Properties Refresh

Hard disks Optical disks Floppy disks

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

Copy Virtual Disk

Storage on physical hard disk

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

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

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

☑ Pre-allocate Full Size

☐ Split into 2GB parts

Back Next Cancel

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

Description:

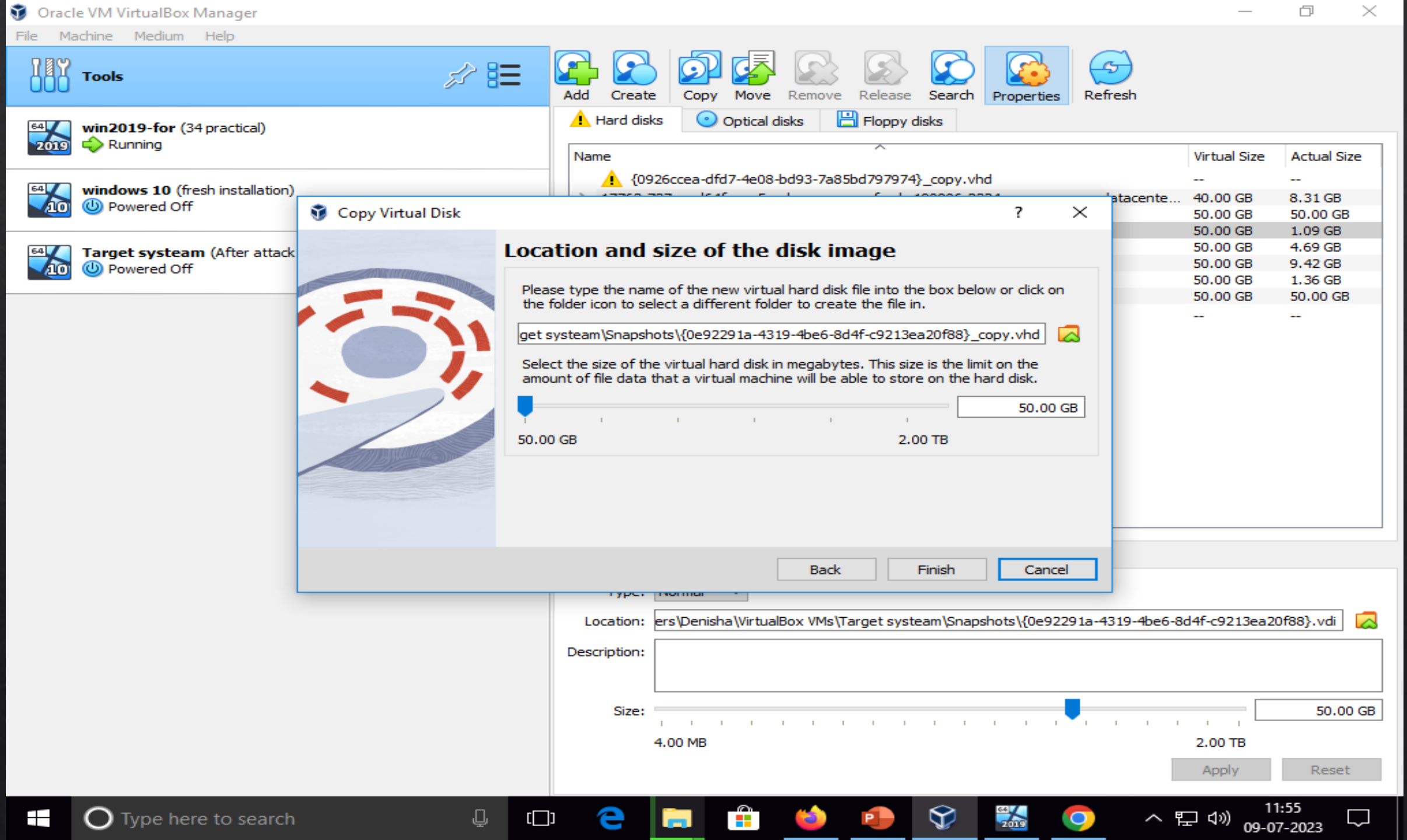
Size: 50.00 GB

4.00 MB 2.00 TB

Apply Reset

Type here to search

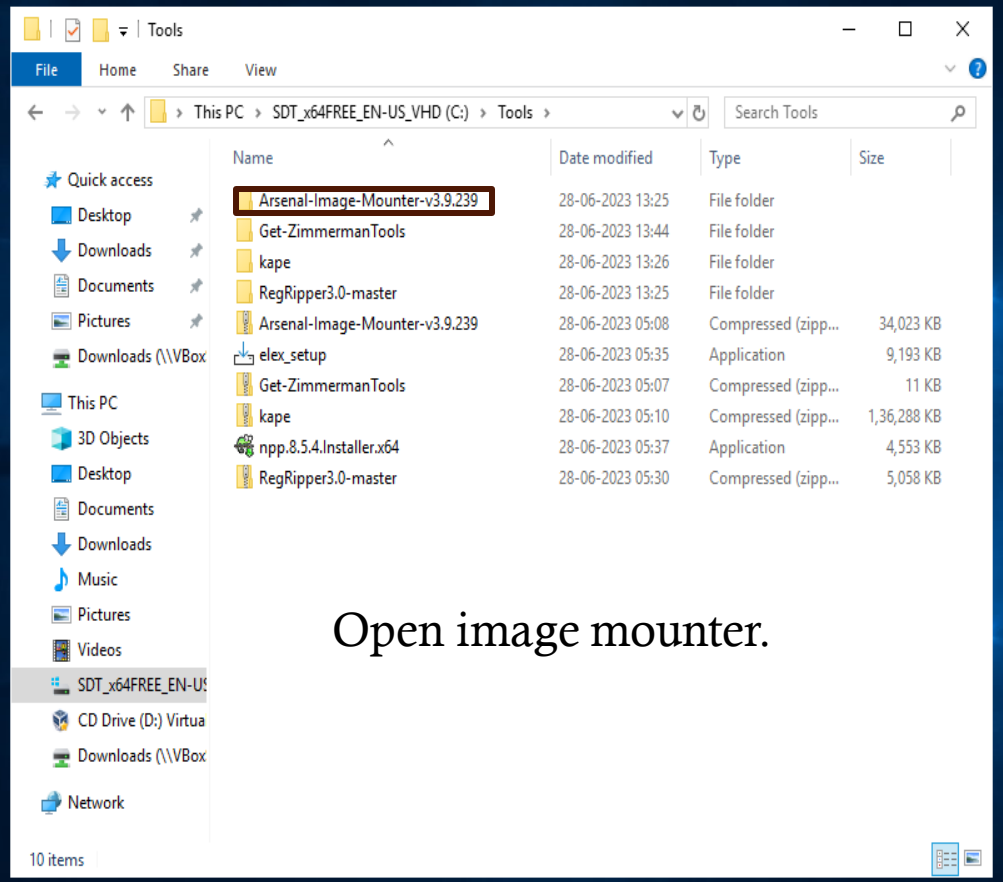
11:54
09-07-2023


Oracle VM VirtualBox Manager
File Machine Medium Help
Tools
win2019-for (34 practical)
Running
windows 10 (fresh installation)
Powered Off
Target systeam (After attack
Powered Off
Add Create Copy Move Remove Release Search Properties Refresh
Hard disks Optical disks Floppy disks
Name Virtual Size Actual Size
{0926ccea-dfd7-4e08-bd93-7a85bd797974}_copy.vhd -- --
40.00 GB 8.31 GB
50.00 GB 50.00 GB
50.00 GB 1.09 GB
50.00 GB 4.69 GB
50.00 GB 9.42 GB
50.00 GB 1.36 GB
50.00 GB 50.00 GB
-- --
Copy Virtual Disk
Location and size of the disk image
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.
get systeam\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.
50.00 GB
50.00 GB 2.00 TB
Back Finish Cancel
Location: ers\Denisha\VirtualBox VMs\Target systeam\Snapshots\{0e92291a-4319-4be6-8d4f-c9213ea20f88}.vdi
Description:
Size: 50.00 GB
4.00 MB 2.00 TB
Apply Reset
Type here to search
11:55
09-07-2023

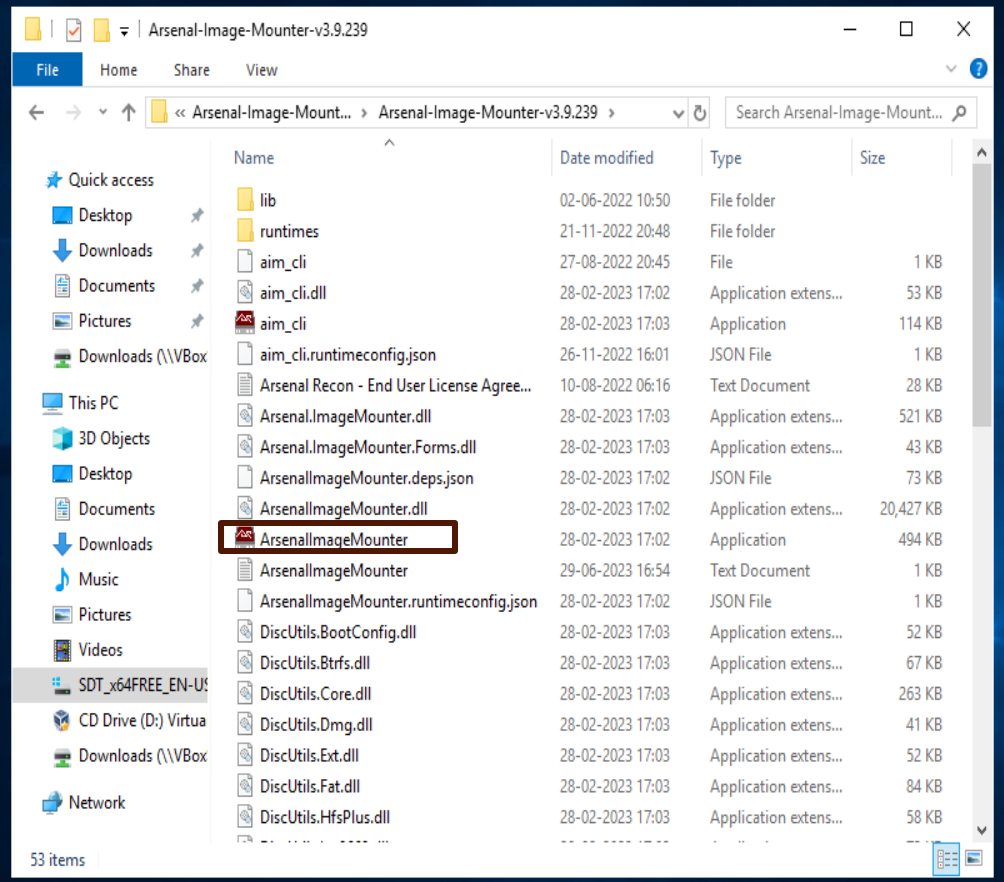
Data Examination

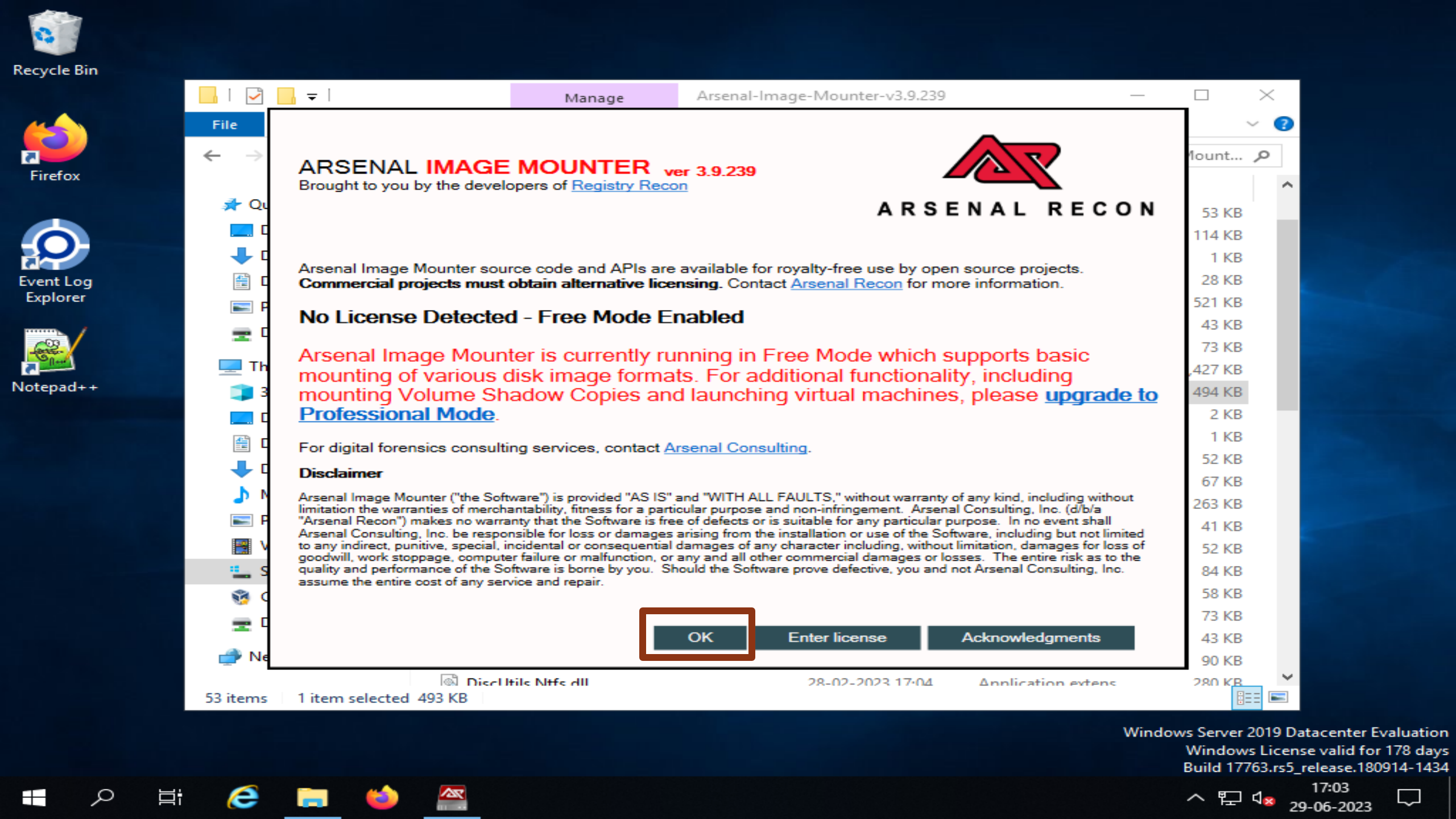
Mounting the disk Image with Arsenal Image Mounter

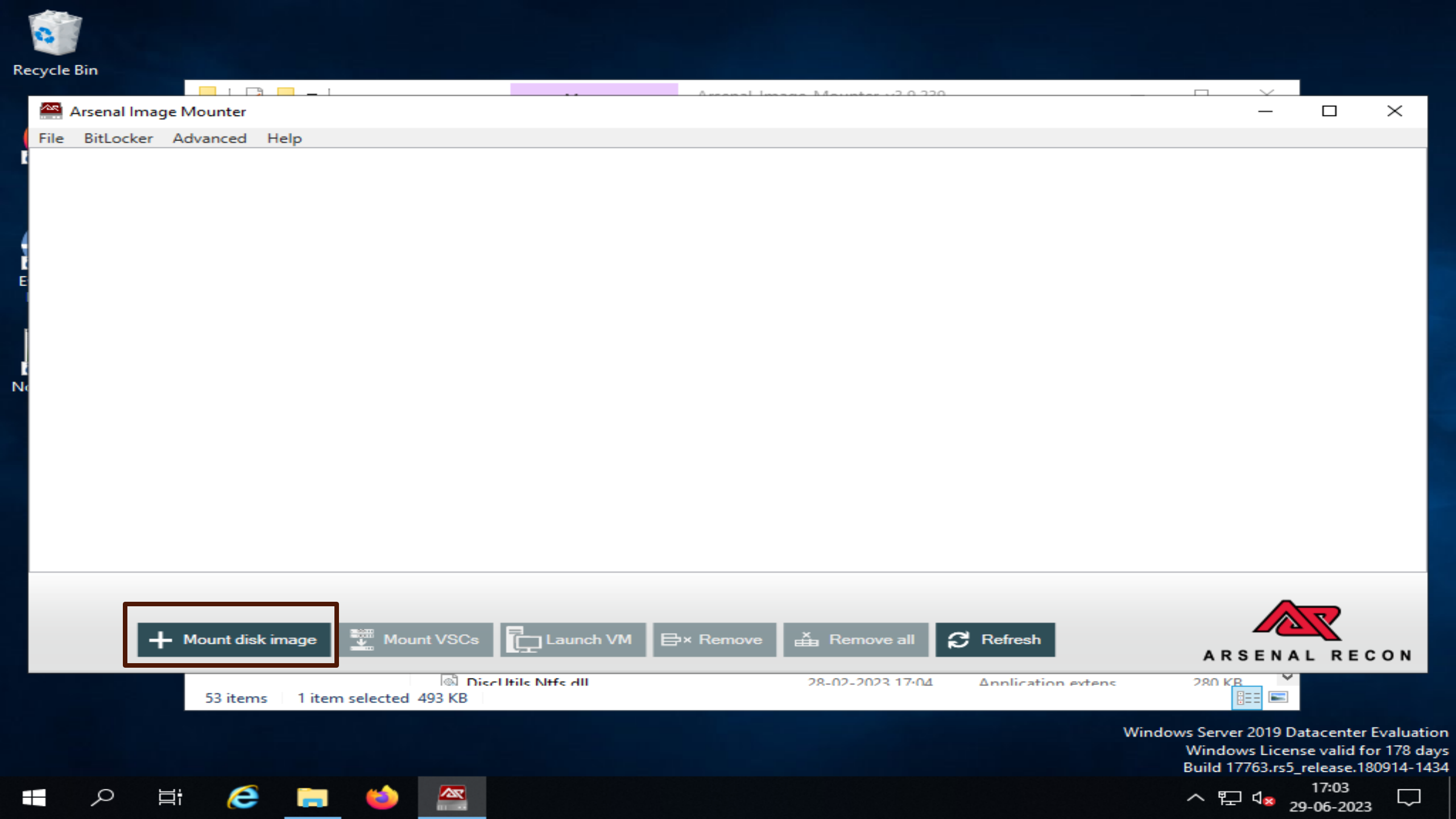
You can enter the Target system harddisk

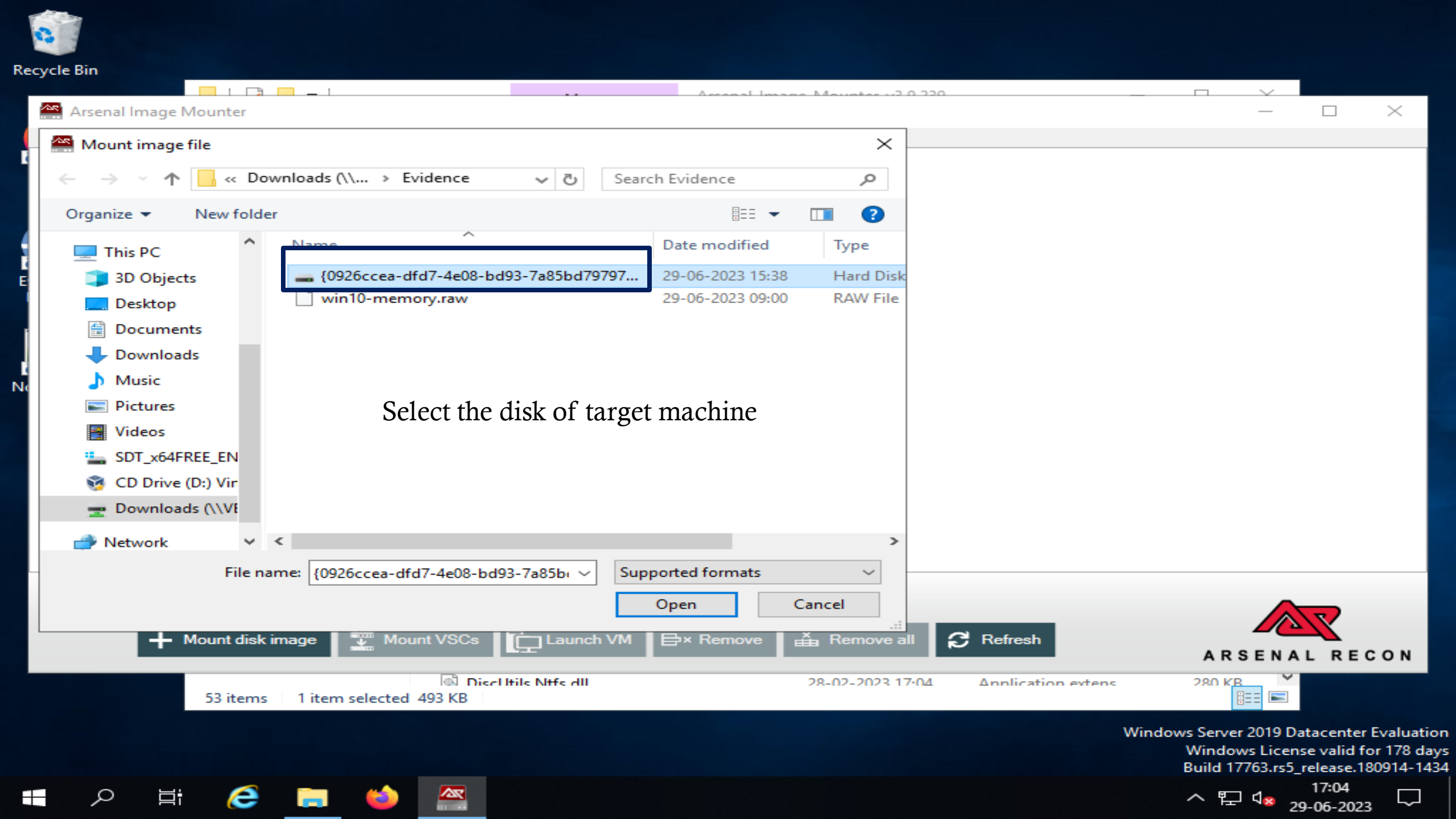


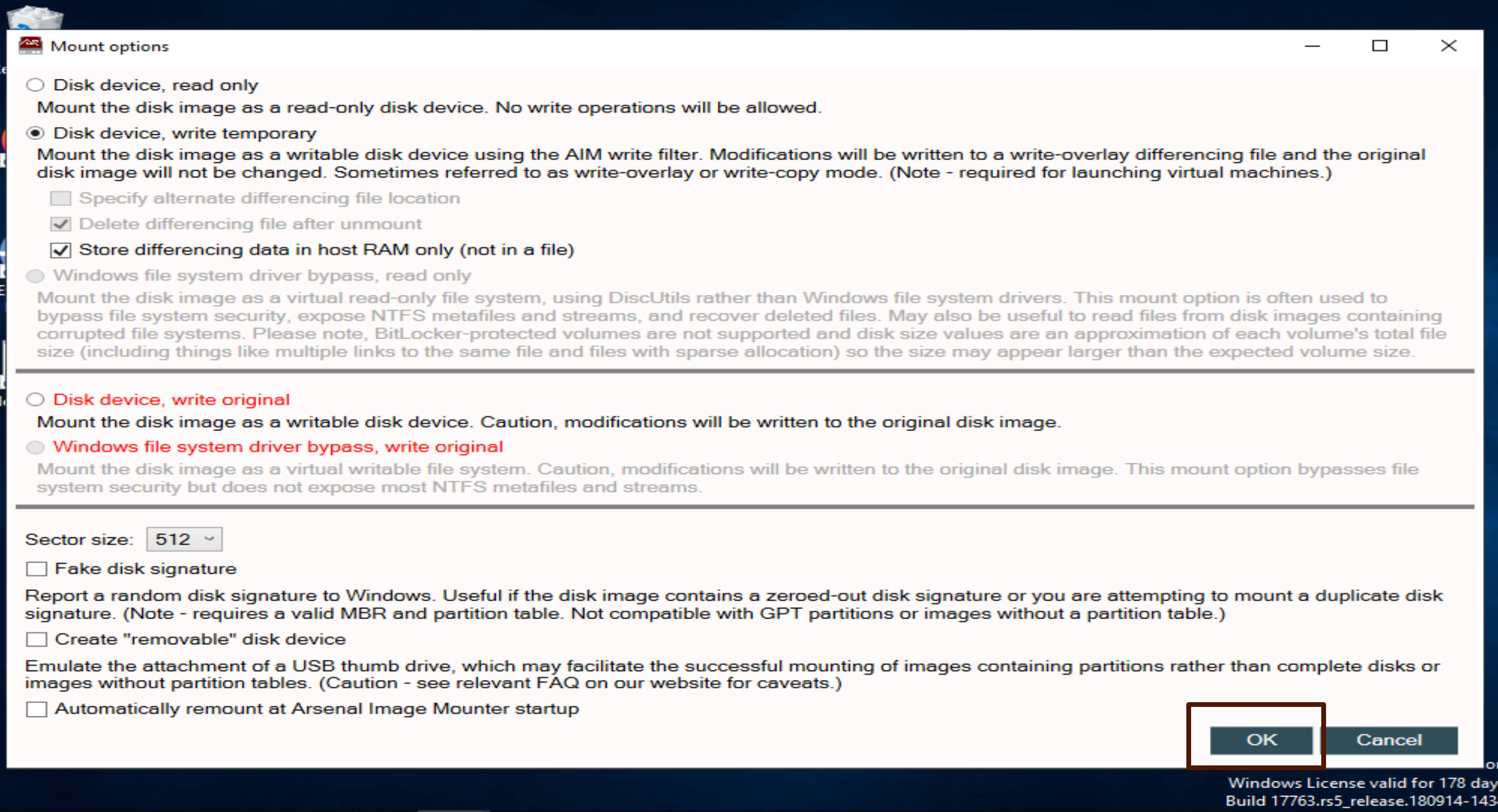
Open image mounter.

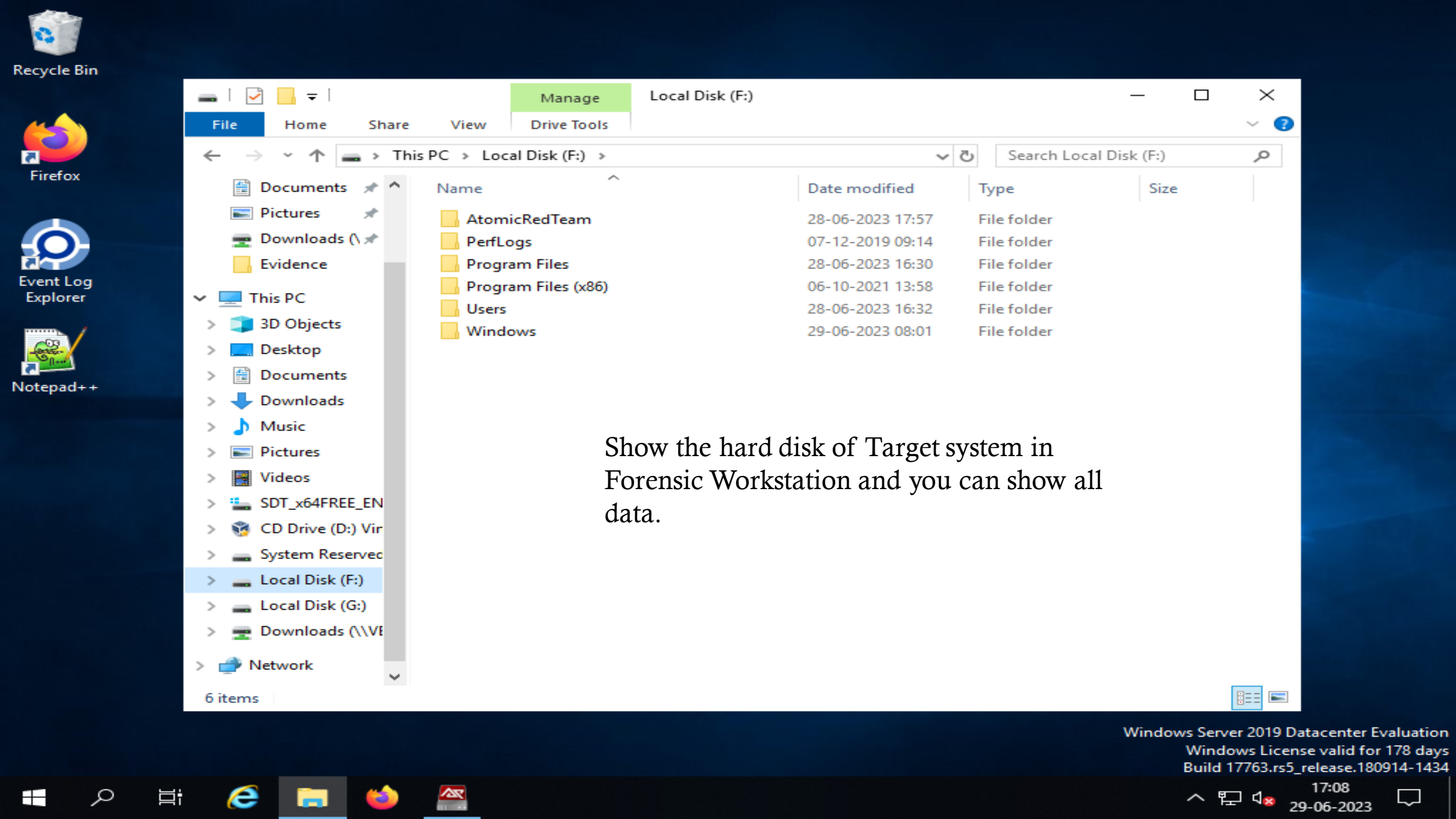



Recycle Bin
Firefox
Event Log Explorer
Notepad++
Manage
Arsenal-Image-Mounter-v3.9.239
File
ARSENAL IMAGE MOUNTER ver 3.9.239
Brought to you by the developers of Registry Recon
ARSENAL RECON
Arsenal Image Mounter source code and APIs are available for royalty-free use by open source projects.
Commercial 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
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
17:03
29-06-2023

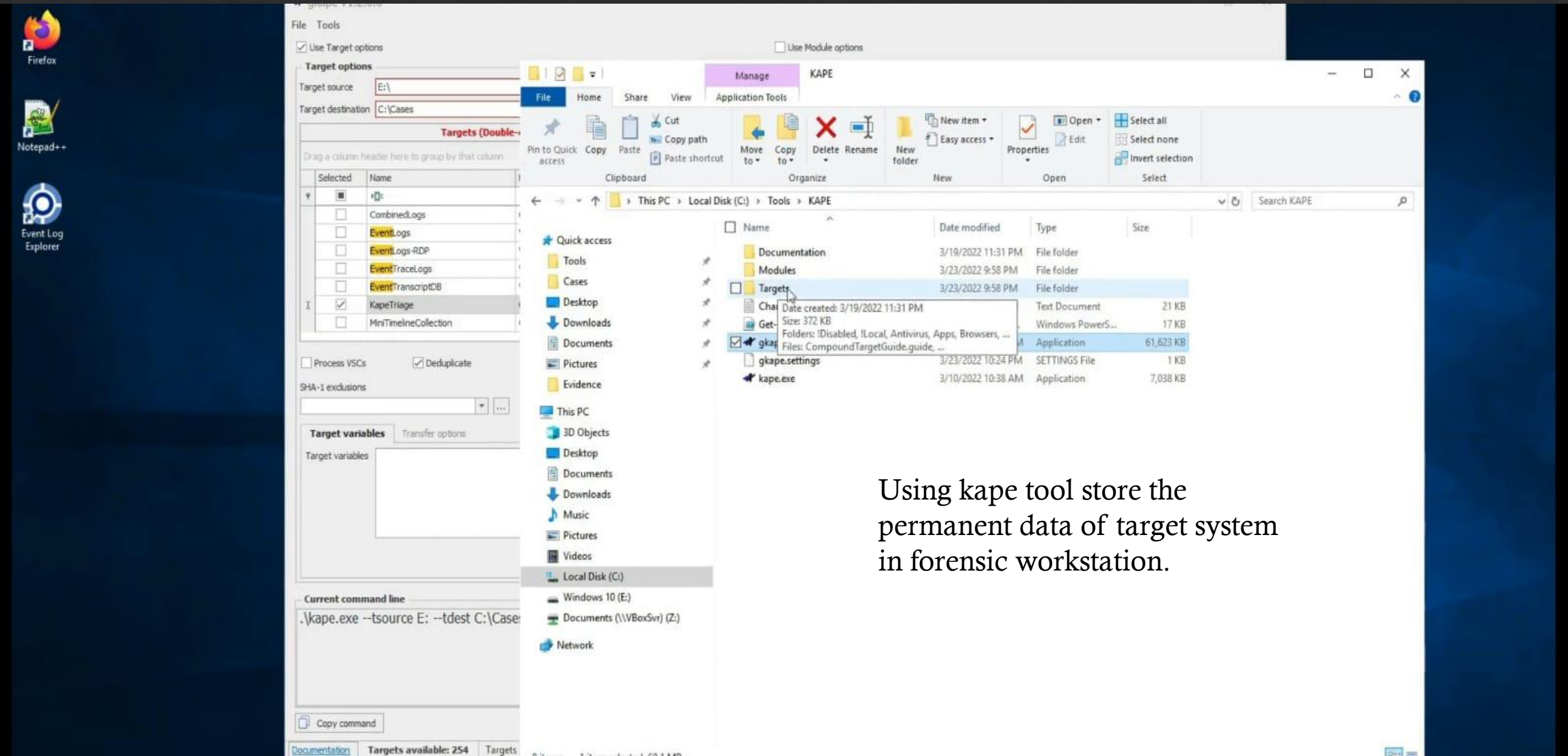

Recycle Bin
Arsenal Image Mounter
File
BitLocker
Advanced
Help
Mount disk image
Mount VSCs
Launch VM
Remove
Remove all
Refresh
ARSENAL RECON
53 items
1 item selected 493 KB
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
17:03
29-06-2023


Recycle Bin
Arsenal Image Mounter
Mount image file
Downloads (\\... › Evidence
Search Evidence
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
SDT_x64FREE_EN
CD Drive (D:) Vir
Downloads (\\VB
Network
Name
Date modified
Type
{0926ccea-dfd7-4e08-bd93-7a85bd79797...
29-06-2023 15:38
Hard Disk
win10-memory.raw
29-06-2023 09:00
RAW File
Select the disk of target machine
File name:
{0926ccea-dfd7-4e08-bd93-7a85b
Supported formats
Open
Cancel
Mount disk image
Mount VSCs
Launch VM
Remove
Remove all
Refresh
ARSENAL RECON
53 items
1 item selected 493 KB
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:
512
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

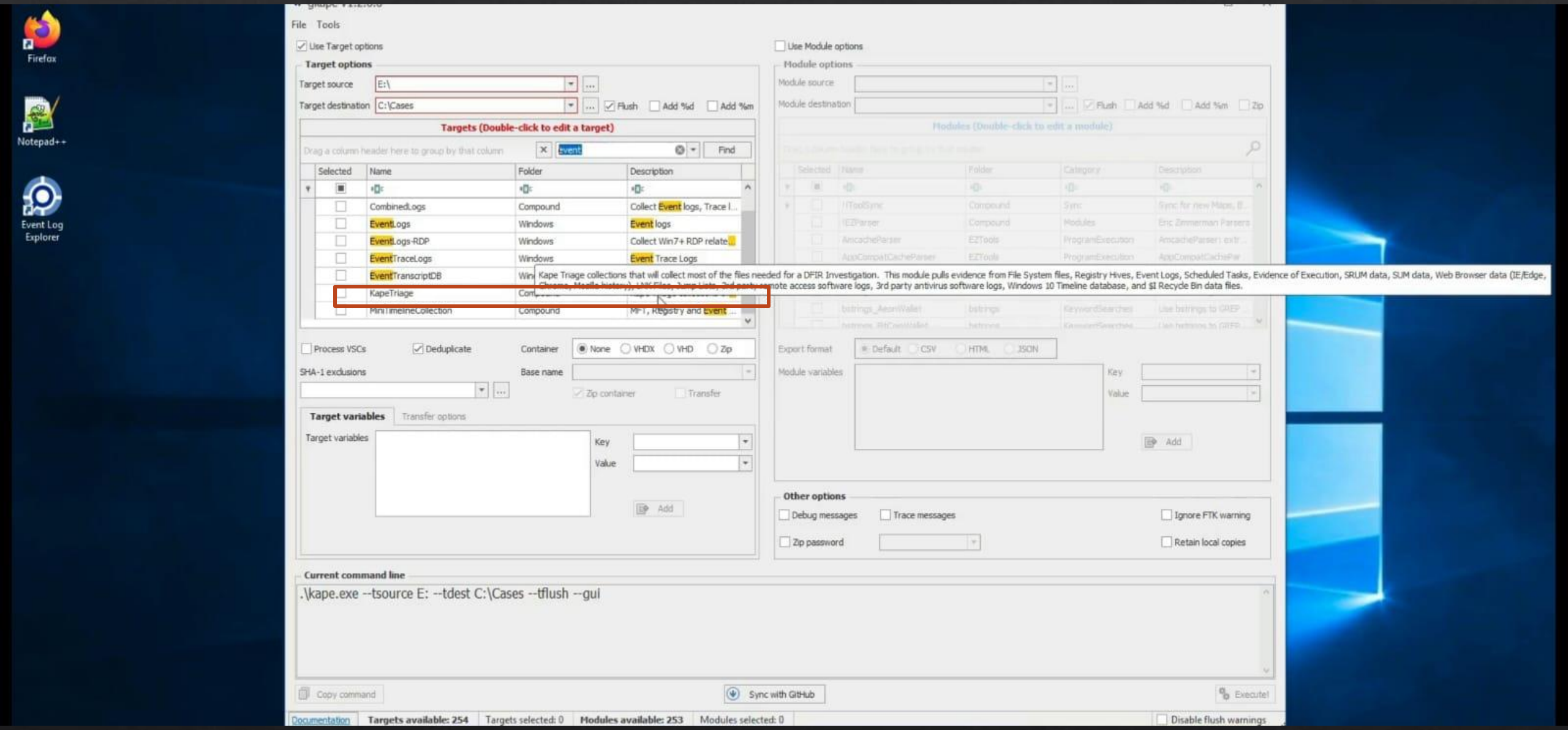

Recycle Bin
Firefox
Event Log Explorer
Notepad++
Manage
Local Disk (F:)
File
Home
Share
View
Drive Tools
This PC › Local Disk (F:) ›
Search Local Disk (F:)
Documents
Pictures
Downloads (\
Evidence
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
SDT_x64FREE_EN
CD Drive (D:) Vir
System Reservec
Local Disk (F:)
Local Disk (G:)
Downloads (\\VE
Network
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
6 items
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

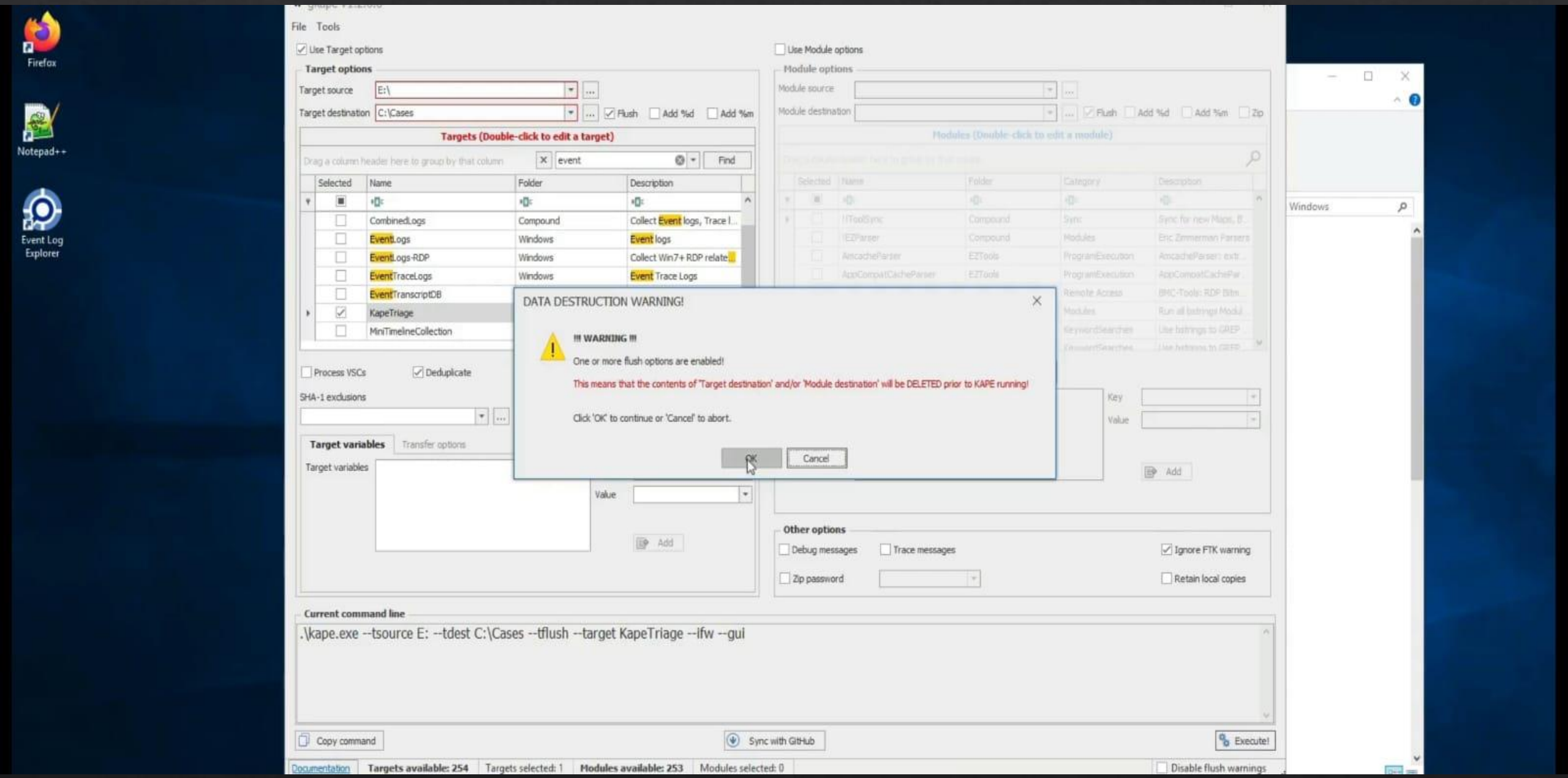
Creating a triage data collection with KAPE Tool

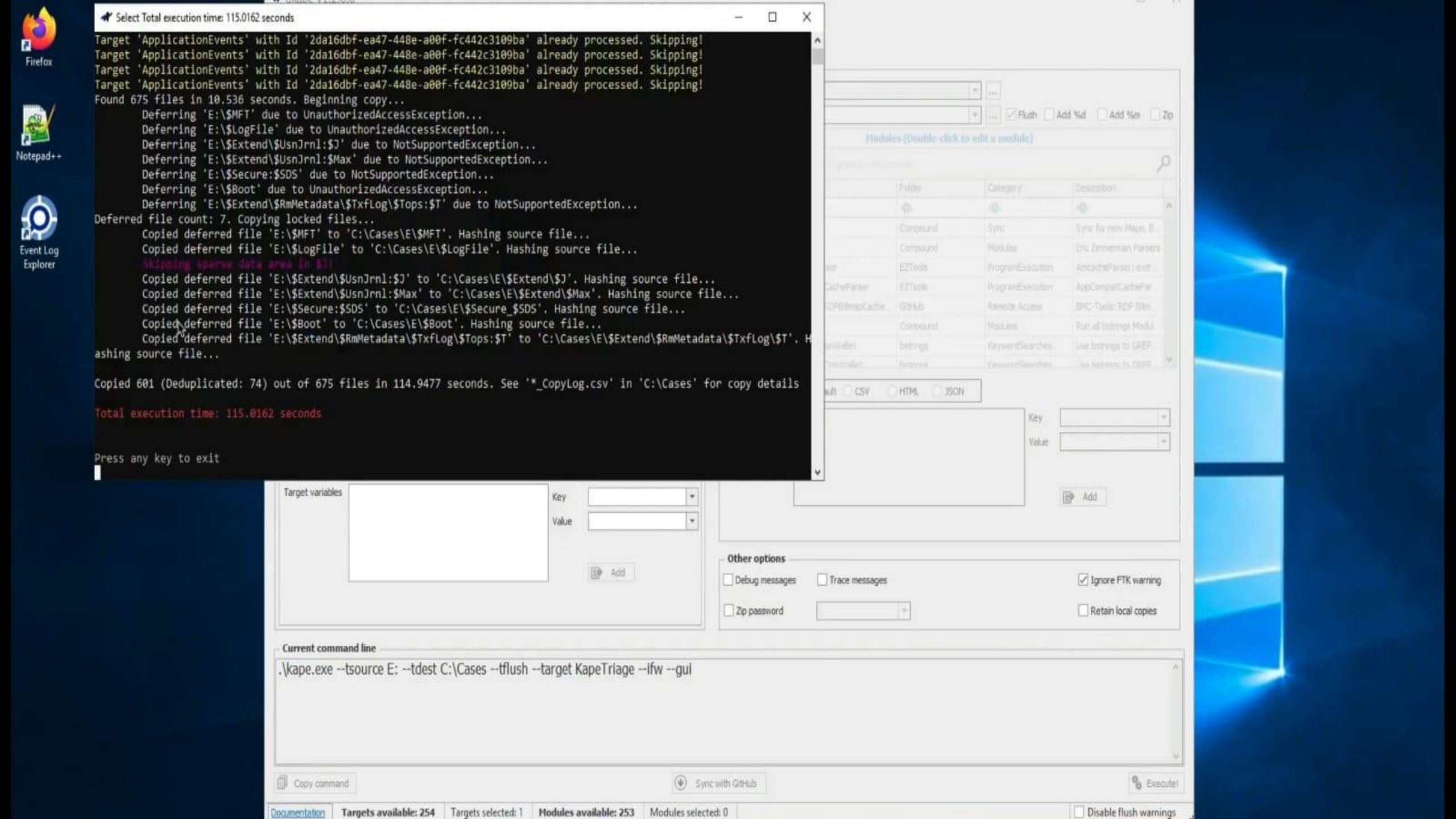


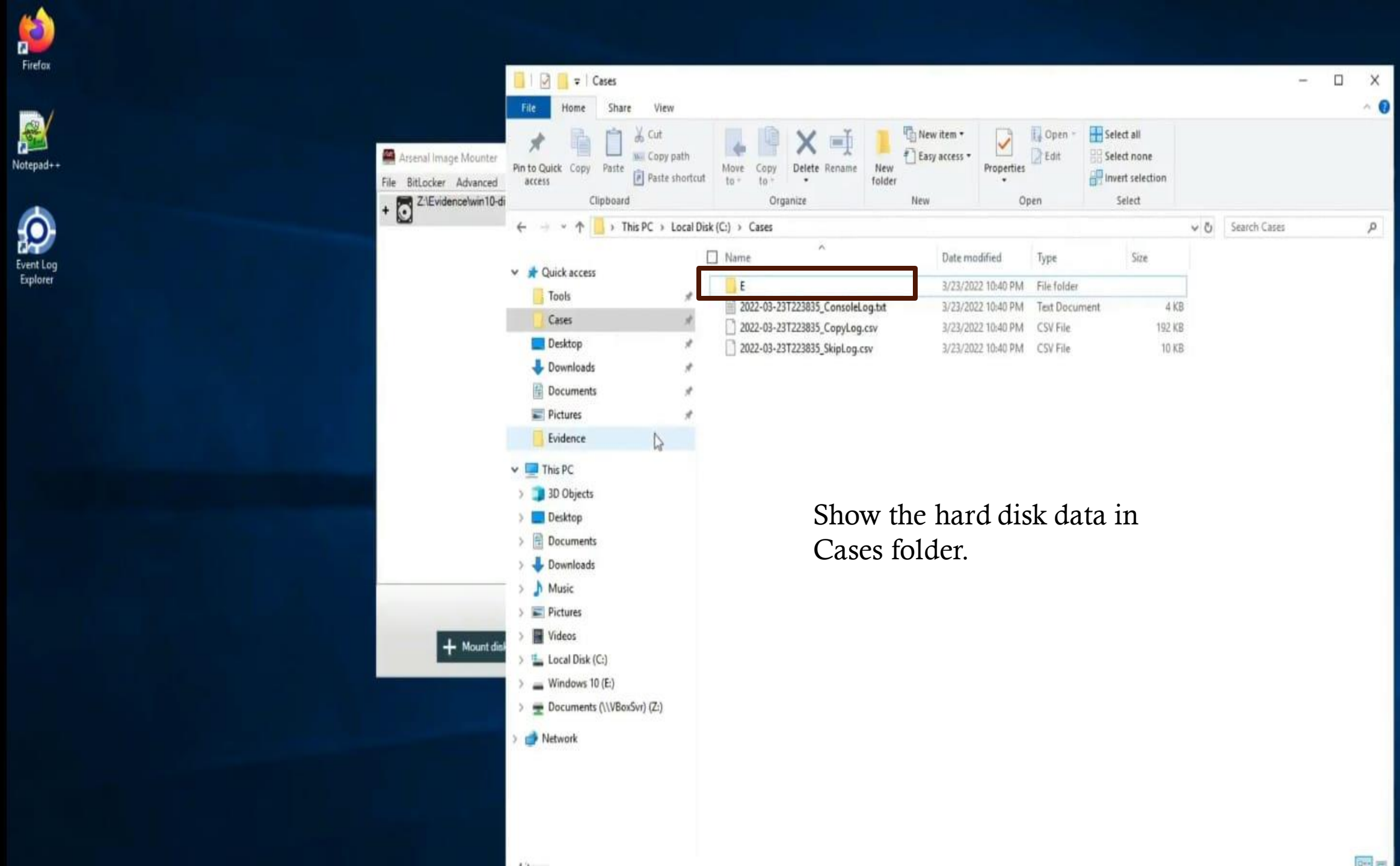
Using kape tool store the permanent data of target system in forensic workstation.

All Data is store in Cases Folder.

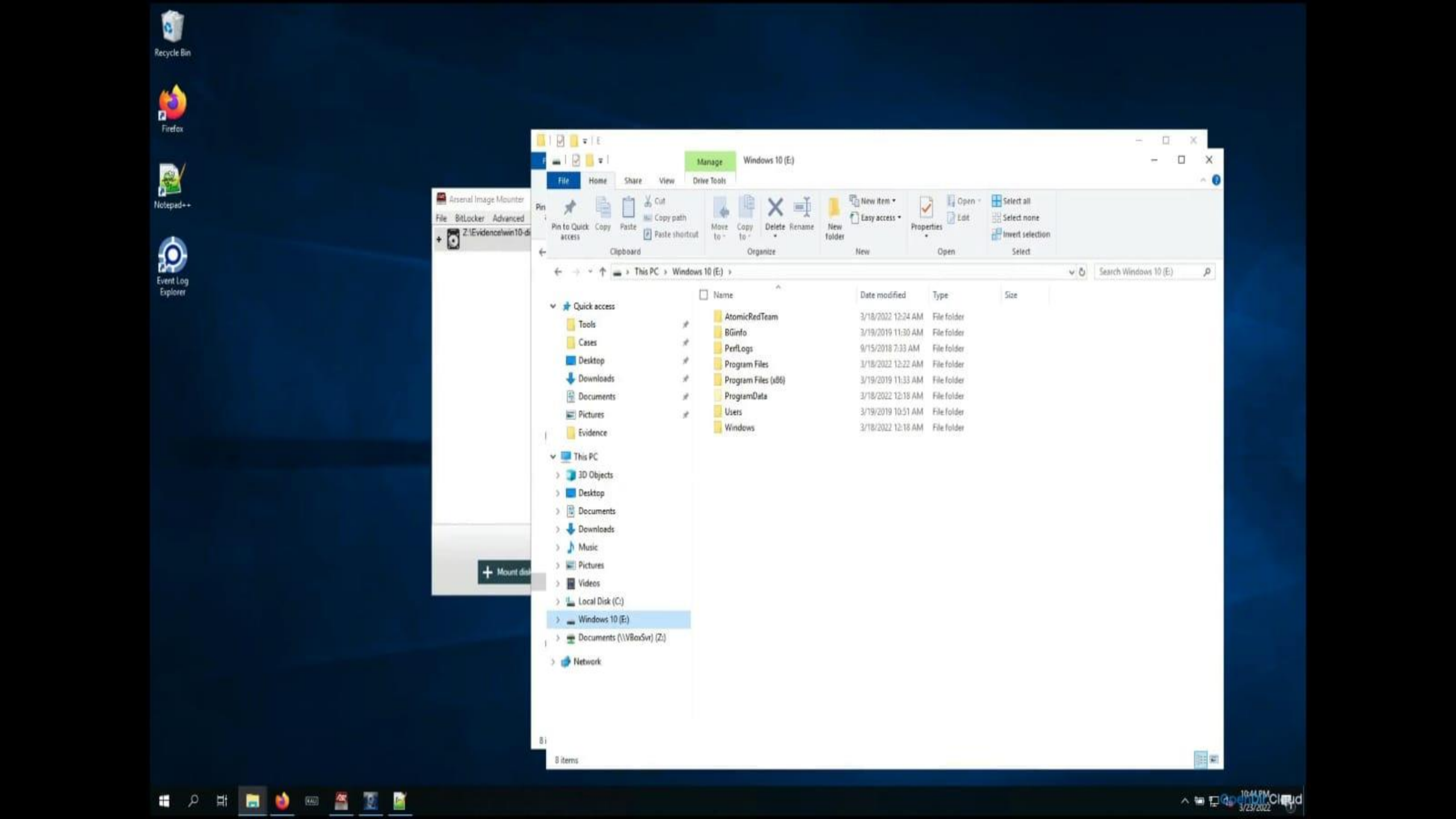



File Tools
Use Target options
Target options
Target source E:\
Target destination C:\Cases
Flush Add %d Add %m
Targets (Double-click to edit a target)
Drag a column header here to group by that column
event
Find
Selected Name Folder Description
CombinedLogs Compound Collect Event logs, Trace l...
EventLogs Windows Event logs
EventLogs-RDP Windows Collect Win7+ RDP relate...
EventTraceLogs Windows Event Trace Logs
EventTranscriptDB
KapeTriage
MiniTimelineCollection
Process VSCs
Deduplicate
SHA-1 exclusions
Target variables
Transfer options
Target variables
Value
Add
Use Module options
Module options
Module source
Module destination
Flush Add %d Add %m Zip
Modules (Double-click to edit a module)
Key
Value
Add
Other options
Debug messages
Trace messages
Ignore FTK warning
Zip password
Retain local copies
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.
OK
Cancel
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
Firefox
Notepad++
Event Log Explorer
Windows


Select Total execution time: 115.0162 seconds
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!
Found 675 files in 10.536 seconds. Beginning copy...
Deferring 'E:\$MFT' due to UnauthorizedAccessException...
Deferring 'E:\$LogFile' due to UnauthorizedAccessException...
Deferring 'E:\$Extend\$UsnJrnl:$J' due to NotSupportedException...
Deferring 'E:\$Extend\$UsnJrnl:$Max' due to NotSupportedException...
Deferring 'E:\$Secure:$SDS' due to NotSupportedException...
Deferring 'E:\$Boot' due to UnauthorizedAccessException...
Deferring 'E:\$Extend\$RmMetadata\$TxfLog\$Tops:$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 $J!
Copied deferred file 'E:\$Extend\$UsnJrnl:$J' to 'C:\Cases\E\$Extend\$J'. Hashing source file...
Copied deferred file 'E:\$Extend\$UsnJrnl:$Max' to 'C:\Cases\E\$Extend\$Max'. Hashing source file...
Copied deferred file 'E:\$Secure:$SDS' to 'C:\Cases\E\$Secure_$SDS'. Hashing source file...
Copied deferred file 'E:\$Boot' to 'C:\Cases\E\$Boot'. Hashing source file...
Copied deferred file 'E:\$Extend\$RmMetadata\$TxfLog\$Tops:$T' to 'C:\Cases\E\$Extend\$RmMetadata\$TxfLog\$T'. H
ashing 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
Firefox
Notepad++
Event Log Explorer
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



Show the hard disk data in Cases folder.


Recycle Bin
Firefox
Notepad++
Event Log Explorer
Arsenal Image Mounter
File BitLocker Advanced
Z:\Evidence\win10-di
Mount disk
Manage
Windows 10 (E:)
File Home Share View Drive Tools
Pin to Quick access Copy Paste Cut Copy path Paste shortcut
Clipboard
Move to Copy to Delete Rename
Organize
New folder New item Easy access
New
Properties Open Edit
Open
Select all Select none Invert selection
Select
This PC › Windows 10 (E:) ›
Search Windows 10 (E:)
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:)
Documents (\\VBoxSvr) (Z:)
Network
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
8 items
10:44 PM
3/23/2022

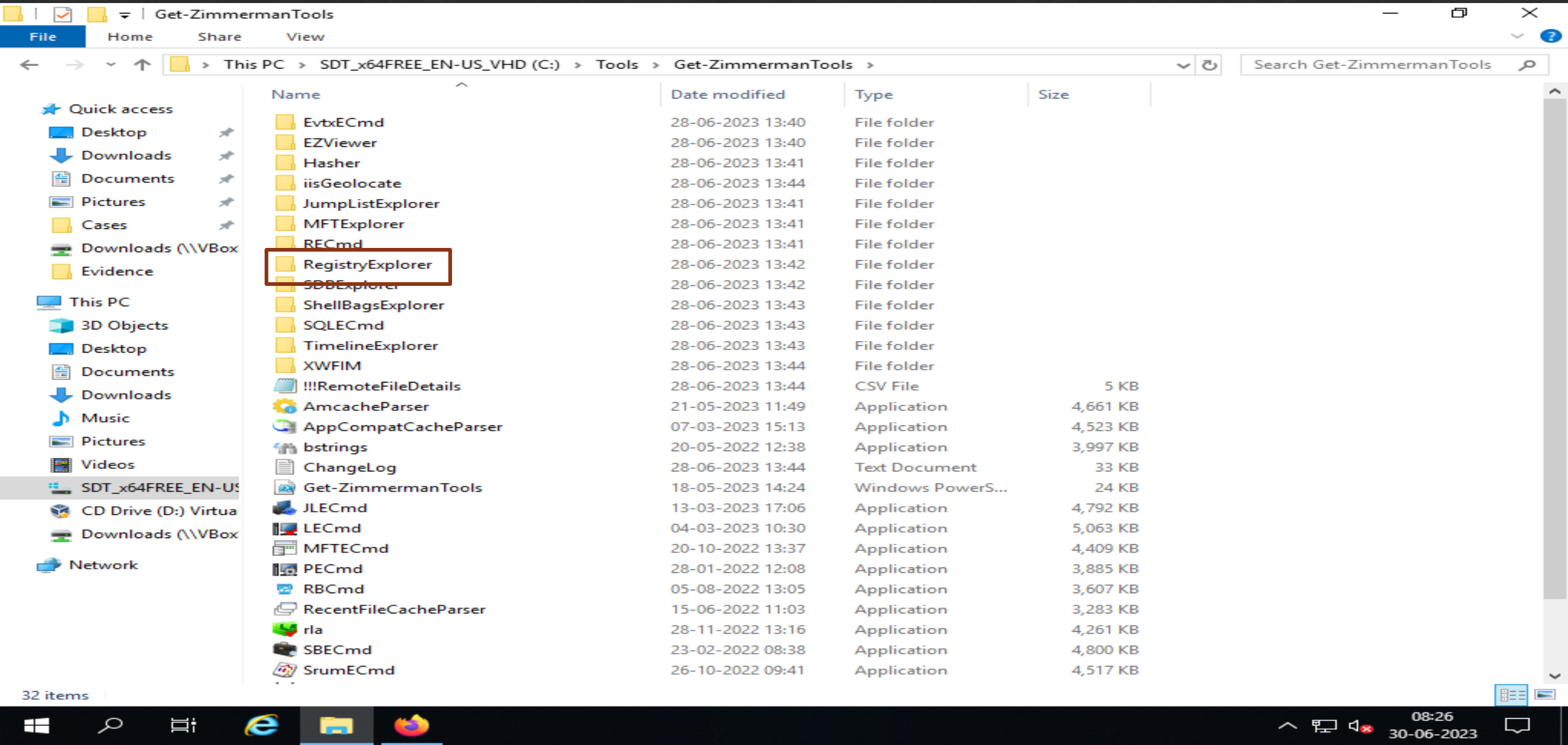
Disk Analysis Process

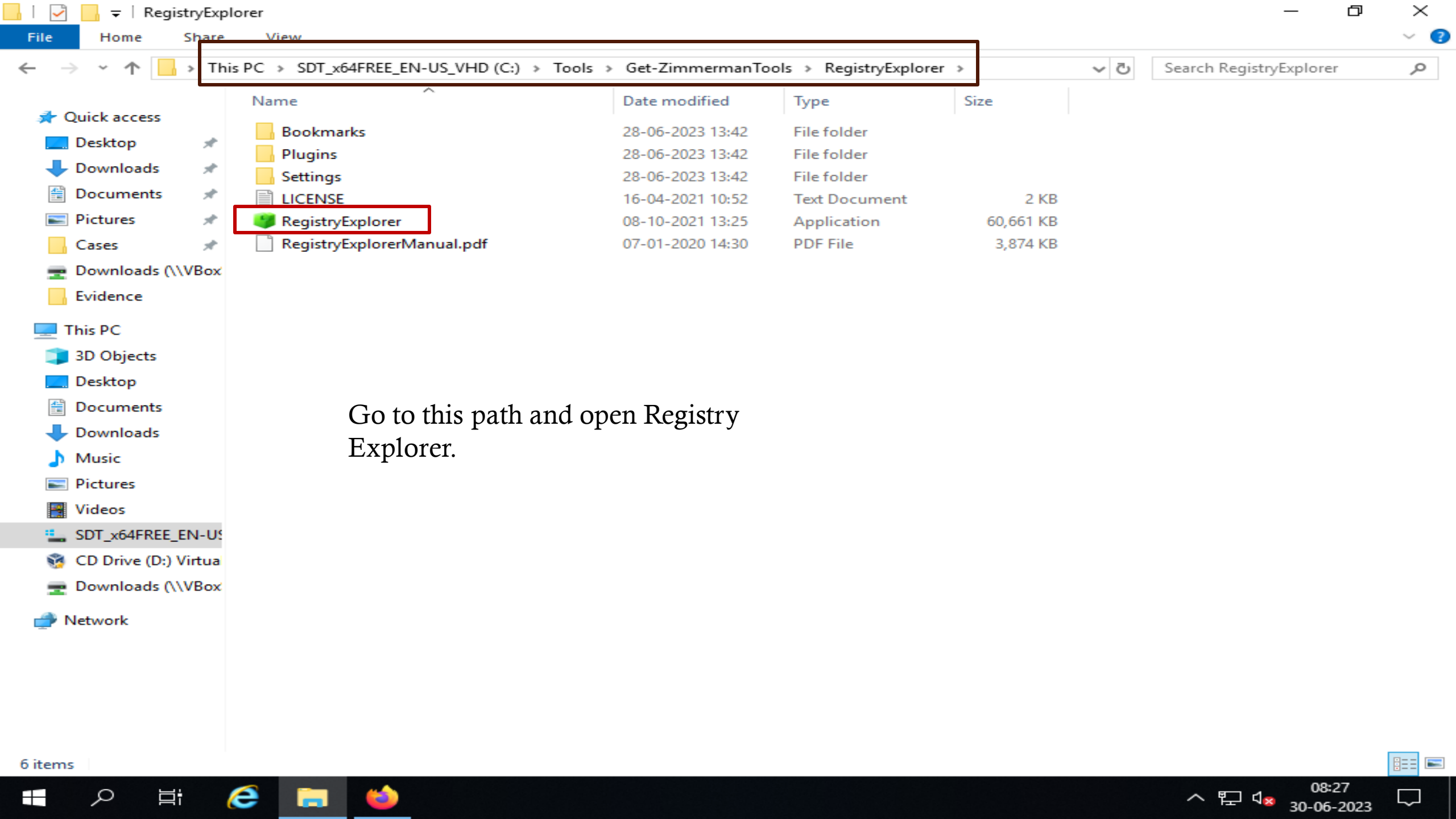
Go to the link and Download the materials.
https://github.com/bluecapesecurity/PWF/blob/main/Resources/Analysis-Notes-Template.docx

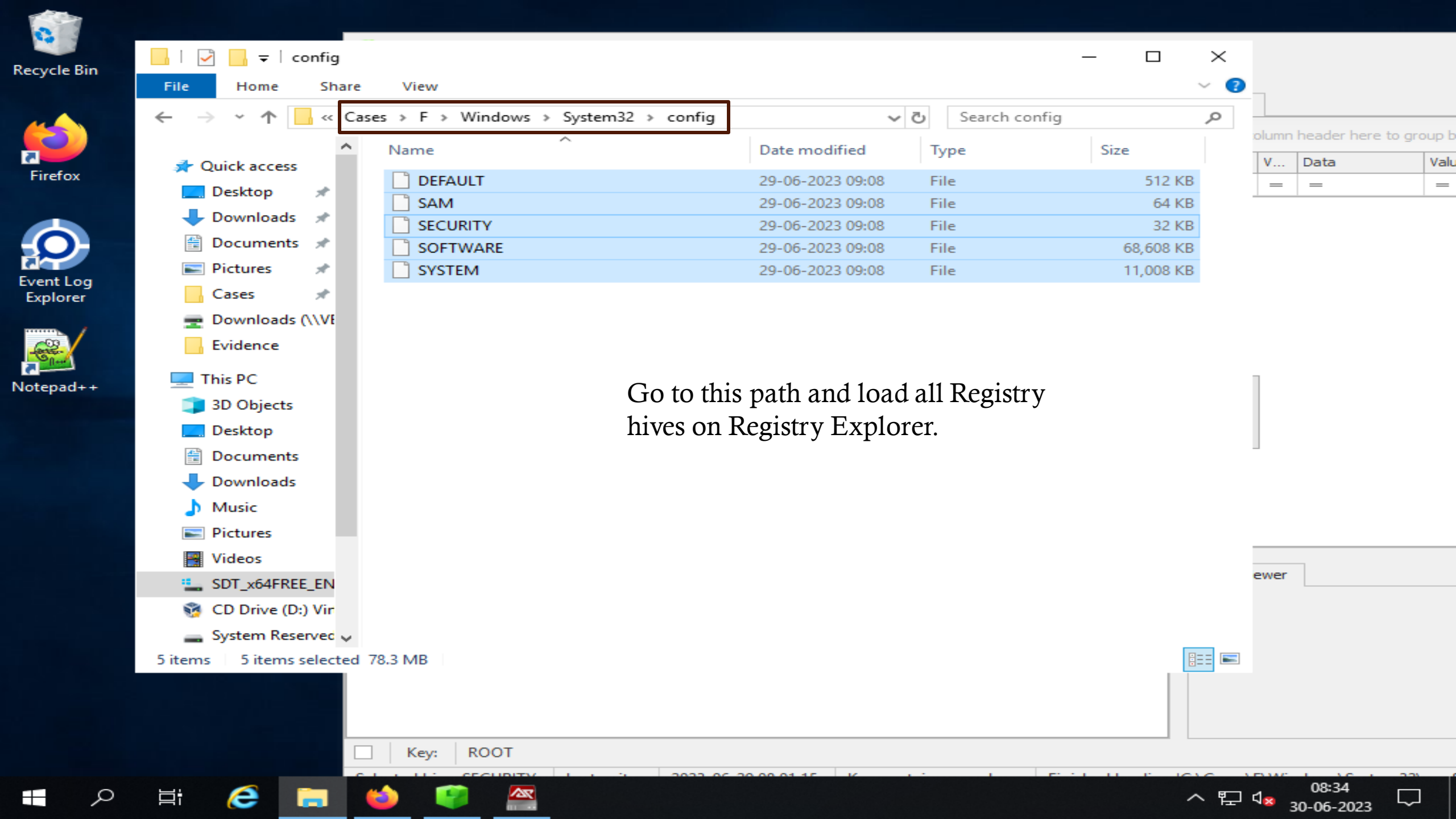
Windows Registry

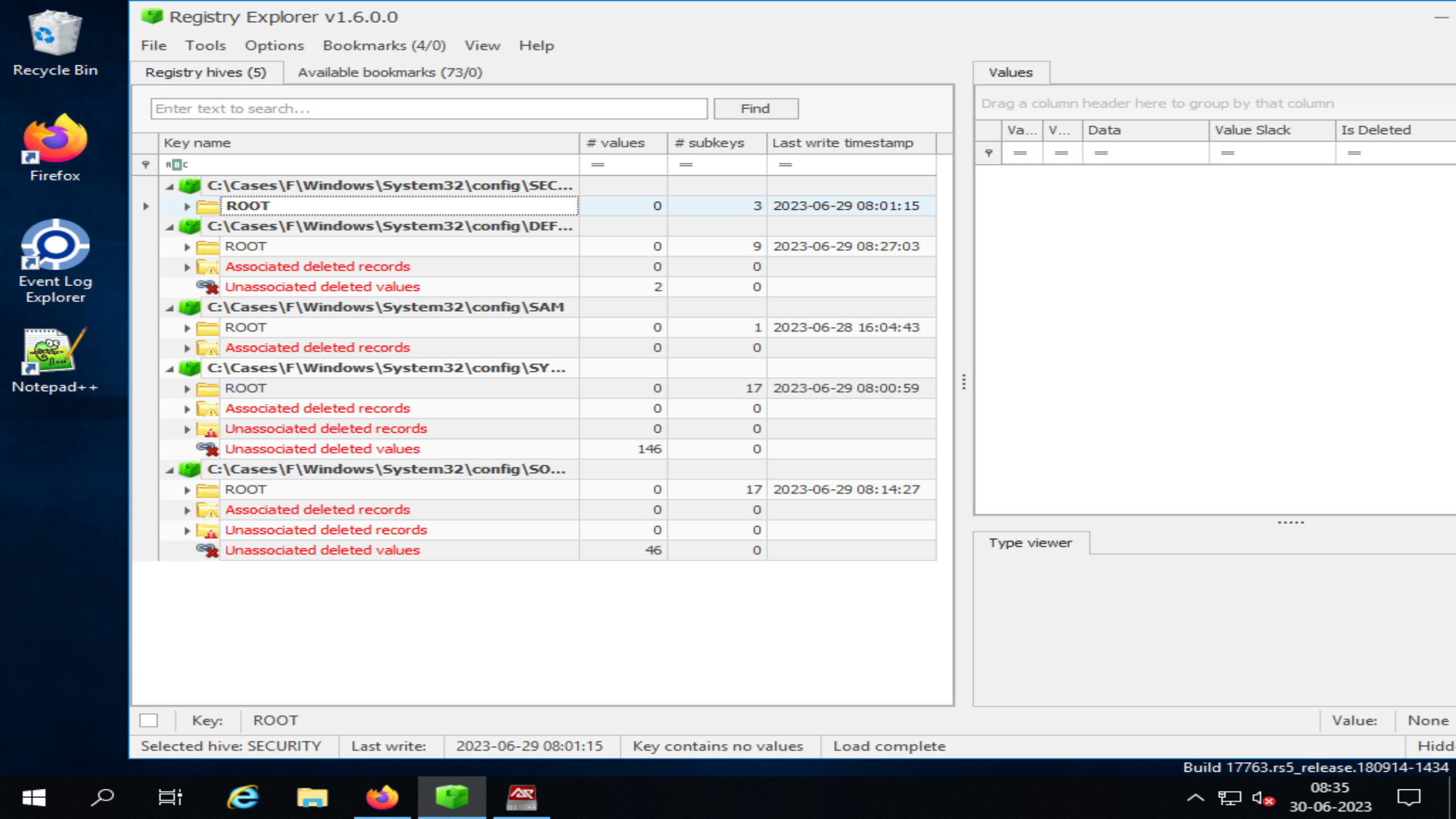
The **registry** or **Windows registry** is a database of information, settings, options, and other values for software and hardware installed on all versions of Microsoft Windows operating systems. When a program is installed, a new subkey is created in the registry. This subkey contains settings specific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

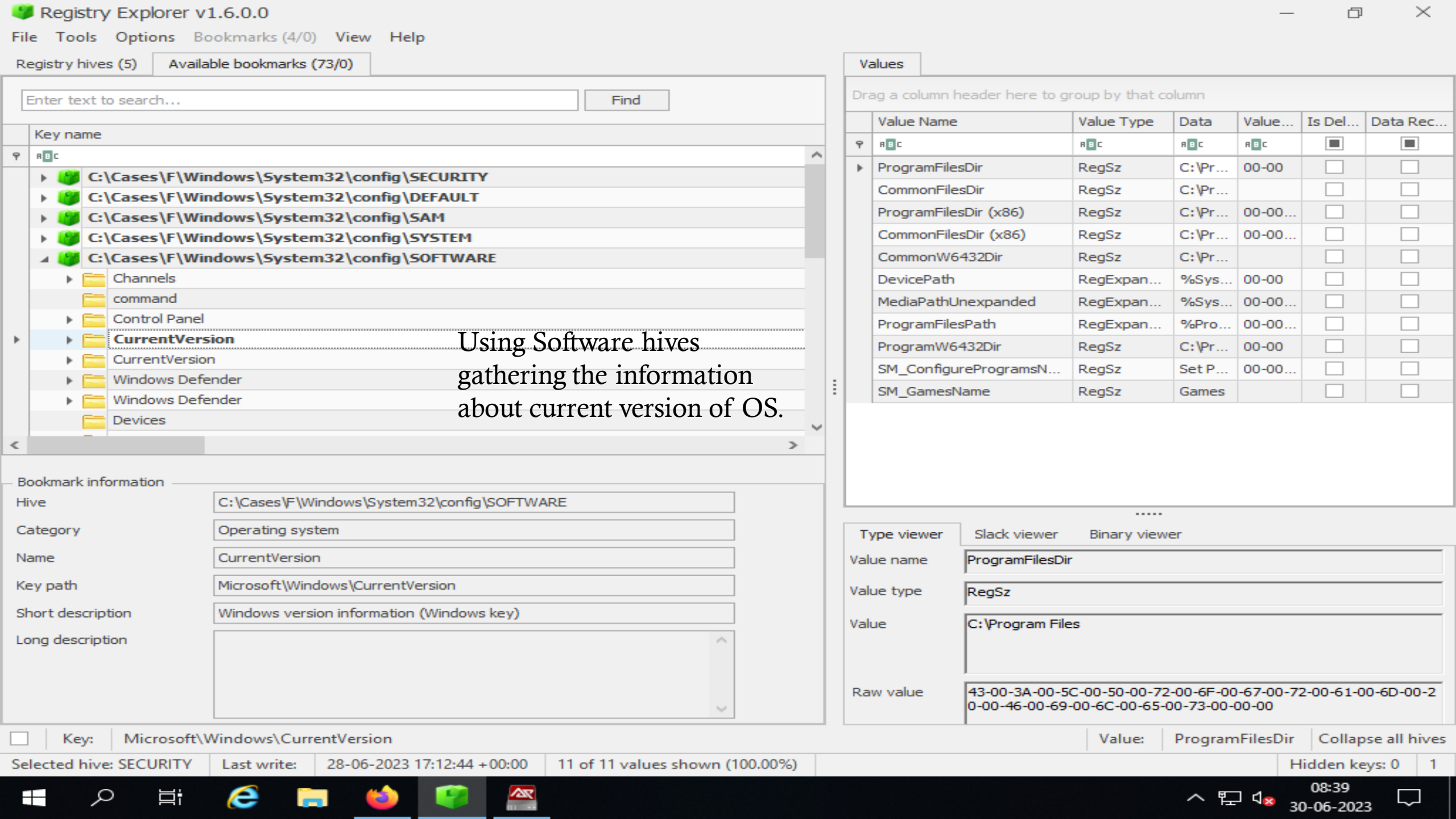
Registry Explorer with Eric Zimmerman Tools

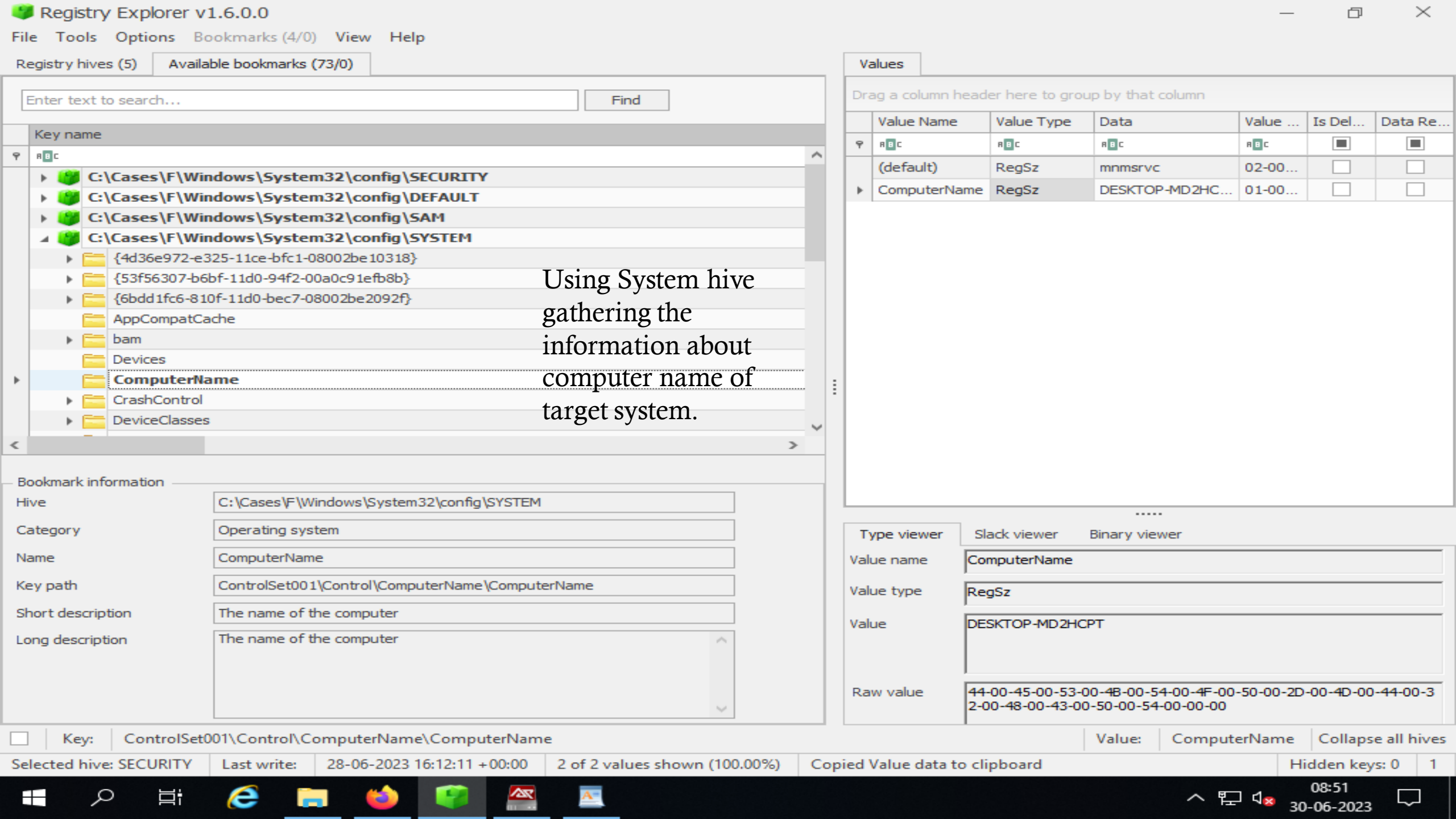



RegistryExplorer
File
Home
Share
View
This PC › SDT_x64FREE_EN-US_VHD (C:) › Tools › Get-ZimmermanTools › RegistryExplorer ›
Search RegistryExplorer
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Downloads (\\VBox
Evidence
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
SDT_x64FREE_EN-US
CD Drive (D:) Virtua
Downloads (\\VBox
Network
Name
Date modified
Type
Size
Bookmarks 28-06-2023 13:42 File folder
Plugins 28-06-2023 13:42 File folder
Settings 28-06-2023 13:42 File folder
LICENSE 16-04-2021 10:52 Text Document 2 KB
RegistryExplorer 08-10-2021 13:25 Application 60,661 KB
RegistryExplorerManual.pdf 07-01-2020 14:30 PDF File 3,874 KB
Go to this path and open Registry Explorer.
6 items
08:27
30-06-2023


Recycle Bin
Firefox
Event Log Explorer
Notepad++
config
File
Home
Share
View
Cases › F › Windows › System32 › config
Search config
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Downloads (\\VE
Evidence
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
SDT_x64FREE_EN
CD Drive (D:) Vir
System Reservec
Name
Date modified
Type
Size
DEFAULT 29-06-2023 09:08 File 512 KB
SAM 29-06-2023 09:08 File 64 KB
SECURITY 29-06-2023 09:08 File 32 KB
SOFTWARE 29-06-2023 09:08 File 68,608 KB
SYSTEM 29-06-2023 09:08 File 11,008 KB
5 items
5 items selected 78.3 MB
Go to this path and load all Registry hives on Registry Explorer.
Key: ROOT
08:34
30-06-2023


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...
ROOT 0 9 2023-06-29 08:27:03
Associated deleted records 0 0
Unassociated deleted values 2 0
C:\Cases\F\Windows\System32\config\SAM
ROOT 0 1 2023-06-28 16:04:43
Associated deleted records 0 0
C:\Cases\F\Windows\System32\config\SY...
ROOT 0 17 2023-06-29 08:00:59
Associated deleted records 0 0
Unassociated deleted records 0 0
Unassociated deleted values 146 0
C:\Cases\F\Windows\System32\config\SO...
ROOT 0 17 2023-06-29 08:14:27
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
Value: None
Selected hive: SECURITY Last write: 2023-06-29 08:01:15 Key contains no values Load complete
Build 17763.rs5_release.180914-1434
08:35
30-06-2023

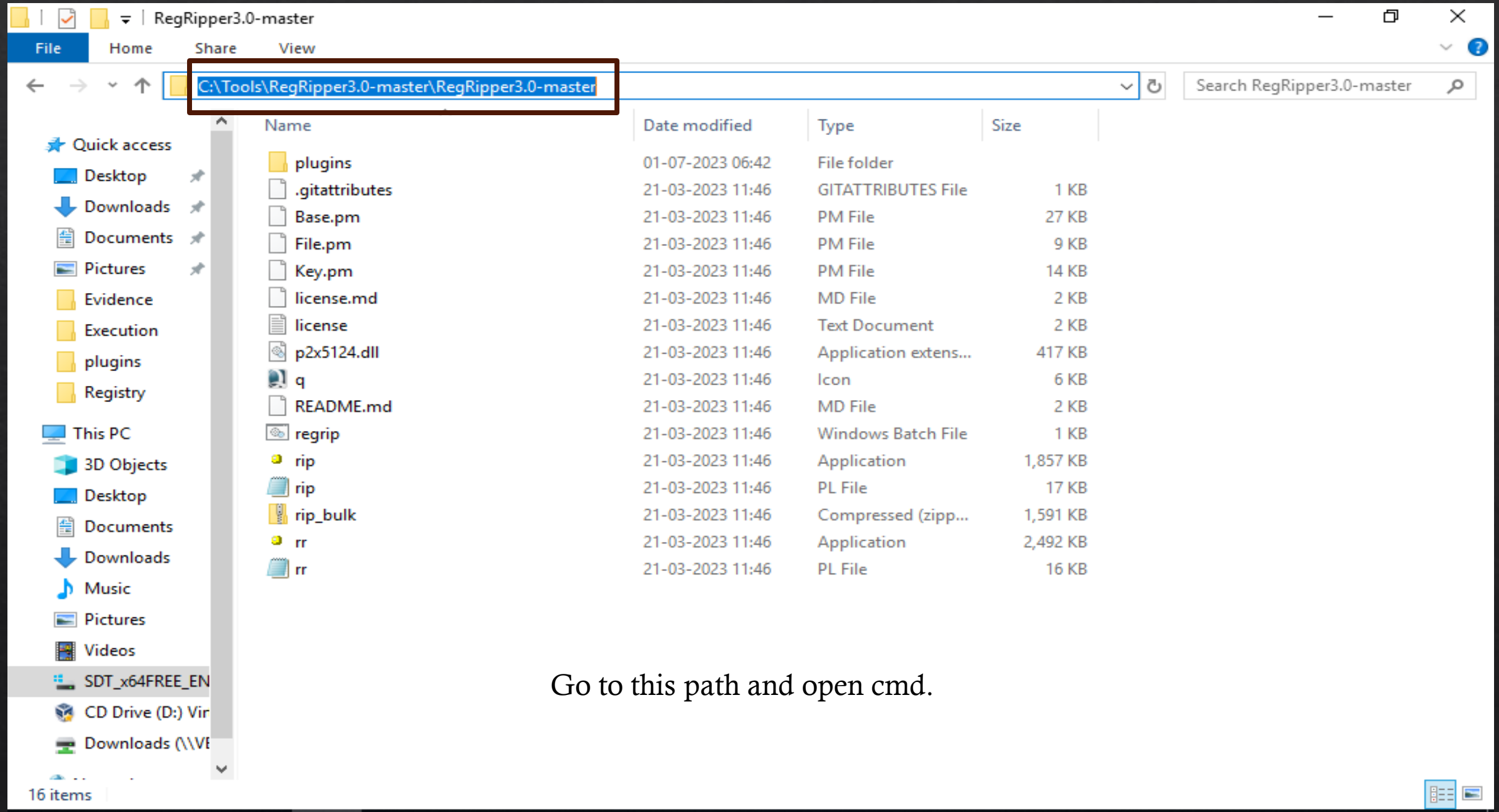

Registry Explorer v1.6.0.0
File Tools Options Bookmarks (4/0) View Help
Registry hives (5) Available bookmarks (73/0)
Enter text to search...
Find
Key name
C:\Cases\F\Windows\System32\config\SECURITY
C:\Cases\F\Windows\System32\config\DEFAULT
C:\Cases\F\Windows\System32\config\SAM
C:\Cases\F\Windows\System32\config\SYSTEM
C:\Cases\F\Windows\System32\config\SOFTWARE
Channels
command
Control Panel
CurrentVersion
CurrentVersion
Windows Defender
Windows Defender
Devices
Using Software hives gathering the information about current version of OS.
Values
Drag a column header here to group by that column
Value Name
Value Type
Data
Value...
Is Del...
Data Rec...
ProgramFilesDir RegSz C:\Pr... 00-00
CommonFilesDir RegSz C:\Pr...
ProgramFilesDir (x86) RegSz C:\Pr... 00-00...
CommonFilesDir (x86) RegSz C:\Pr... 00-00...
CommonW6432Dir RegSz C:\Pr...
DevicePath RegExpan... %Sys... 00-00
MediaPathUnexpanded RegExpan... %Sys... 00-00...
ProgramFilesPath RegExpan... %Pro... 00-00...
ProgramW6432Dir RegSz C:\Pr... 00-00
SM_ConfigureProgramsN... RegSz Set P... 00-00...
SM_GamesName RegSz Games
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
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
Key: Microsoft\Windows\CurrentVersion
Value: ProgramFilesDir
Collapse all hives
Selected hive: SECURITY
Last write: 28-06-2023 17:12:44 +00:00
11 of 11 values shown (100.00%)
Hidden keys: 0
1
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
C:\Cases\F\Windows\System32\config\SECURITY
C:\Cases\F\Windows\System32\config\DEFAULT
C:\Cases\F\Windows\System32\config\SAM
C:\Cases\F\Windows\System32\config\SYSTEM
{4d36e972-e325-11ce-bfc1-08002be10318}
{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
{6bdd1fc6-810f-11d0-bec7-08002be2092f}
AppCompatCache
bam
Devices
ComputerName
CrashControl
DeviceClasses
Using System hive gathering the information about computer name of target system.
Values
Drag a column header here to group by that column
Value Name
Value Type
Data
Value ...
Is Del...
Data Re...
(default)
RegSz
mnmsrvc
02-00...
ComputerName
RegSz
DESKTOP-MD2HC...
01-00...
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
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

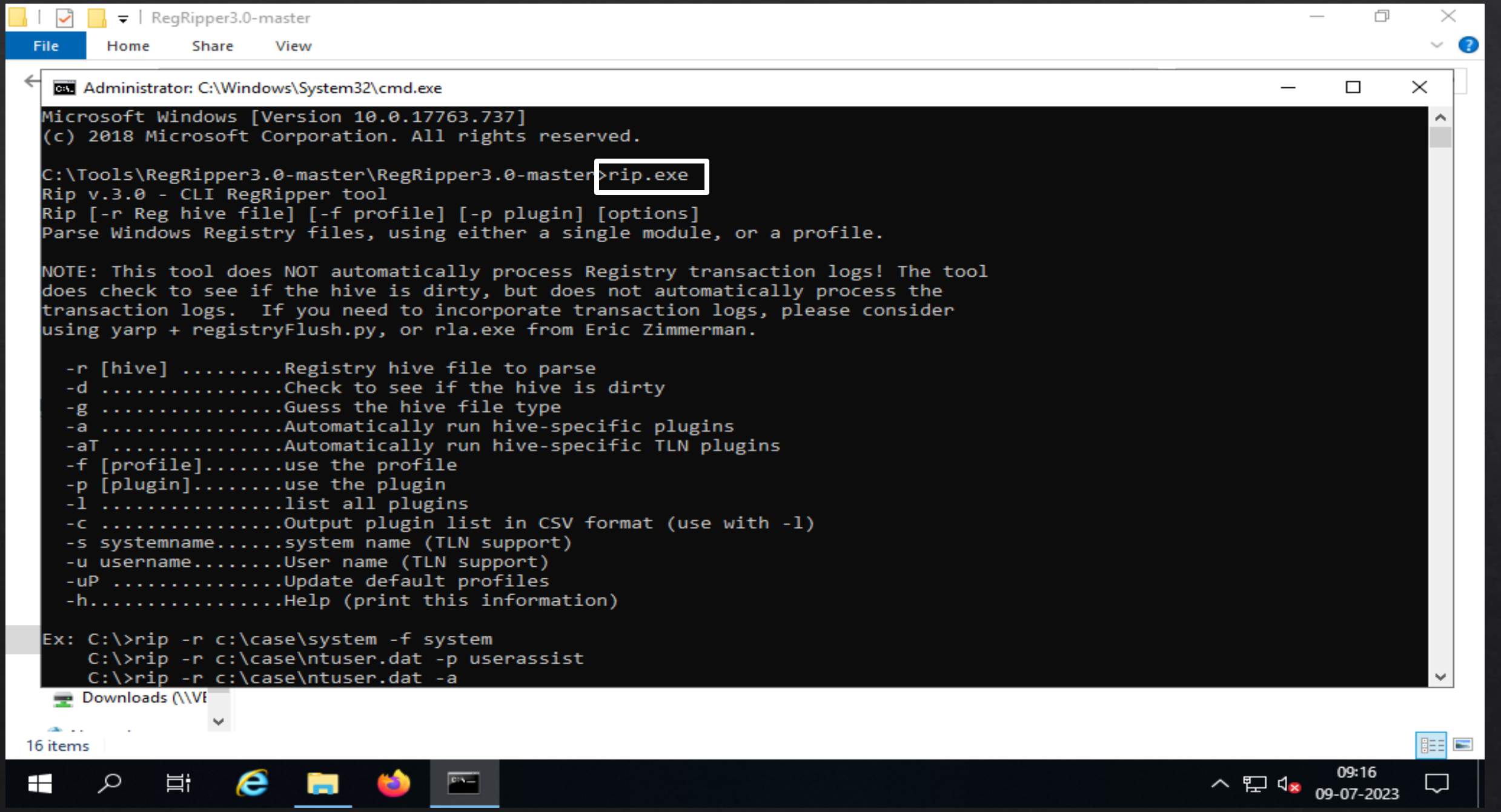
Gathering system information with RegRipper

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



Go to this path and open cmd.


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 (\\VE
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.

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.

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

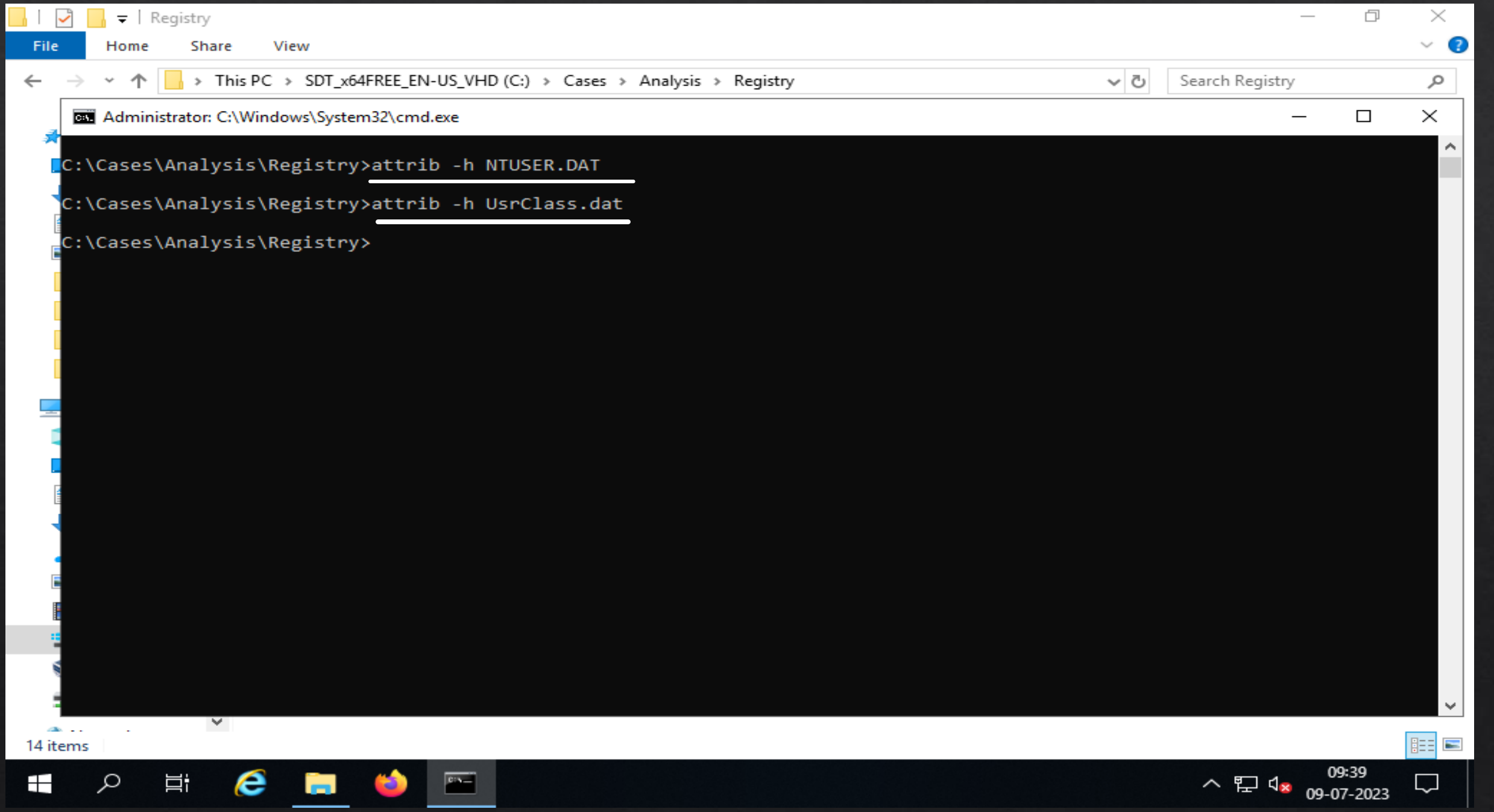
```
ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.

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

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

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
```

Detail about last shutdown time of target system.

Detail about Microsoft defender

Parsing registry hives in bulk with RegRipper

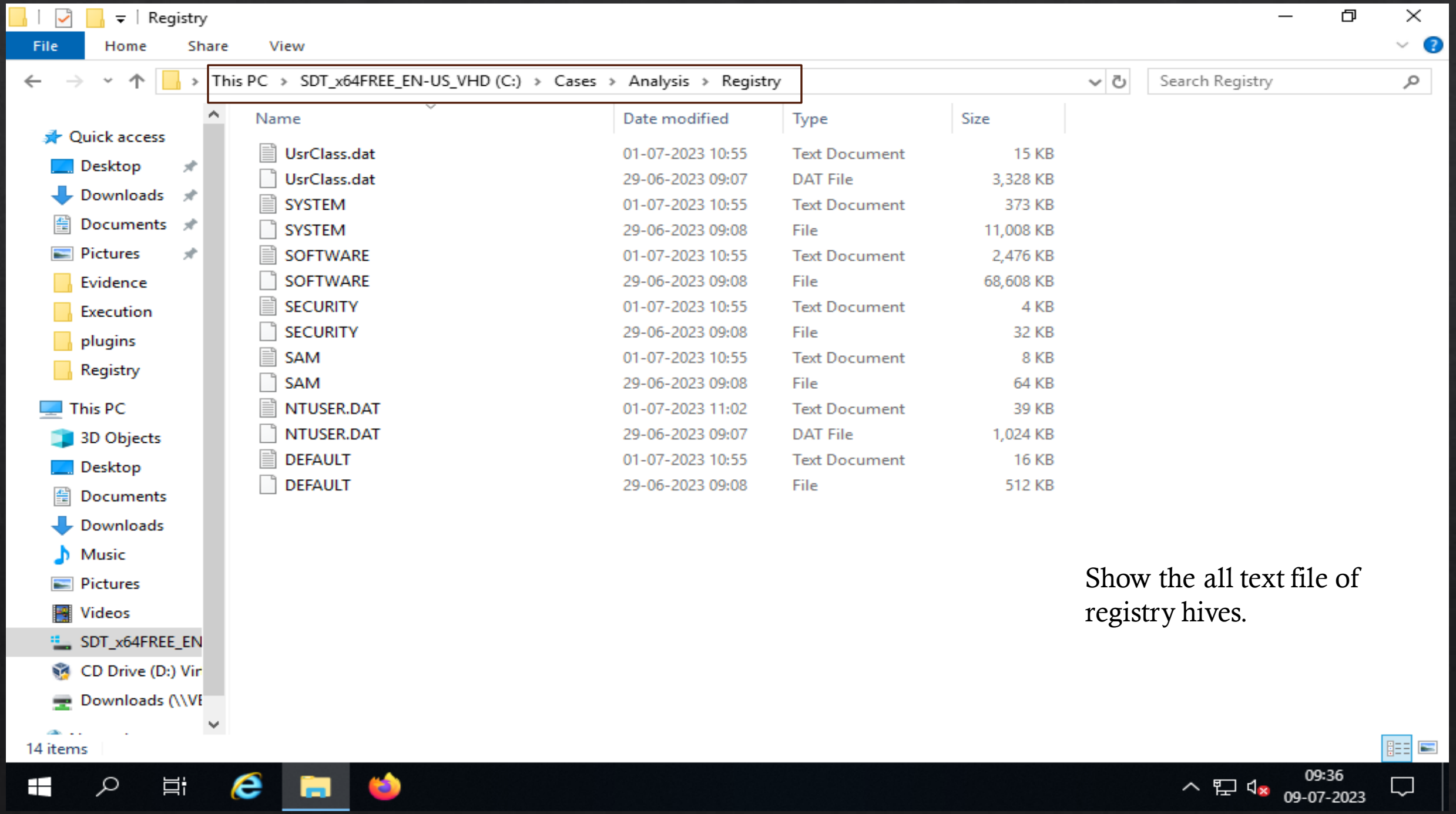
1. Go to the Registry folder location > open cmd > dir > attrib * > attrib –h NTUSER>DAT > attrib –h UserClass.dat
2. For /r %i in (*) do (C:\Tools\RegRipper\rip.exe –r %i –a > %i.txt).
3. Show in Registry folder text file automatic created then after all file selected and edit with Notepad++ and show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


Registry
File
Home
Share
View
This PC
SDT_x64FREE_EN-US_VHD (C:)
Cases
Analysis
Registry
Search Registry
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

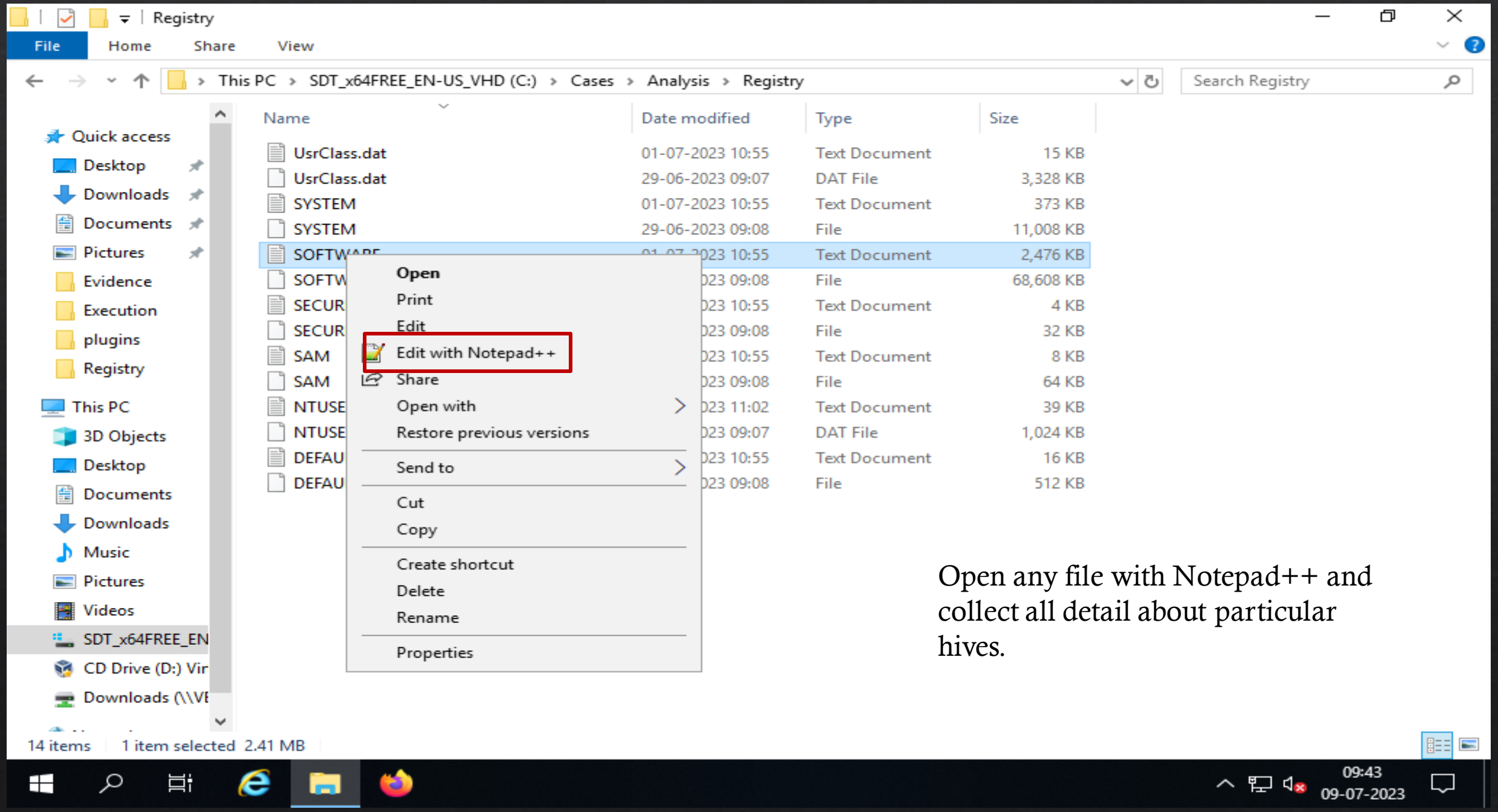
Administrator: C:\Windows\System32\cmd.exe

```
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
```

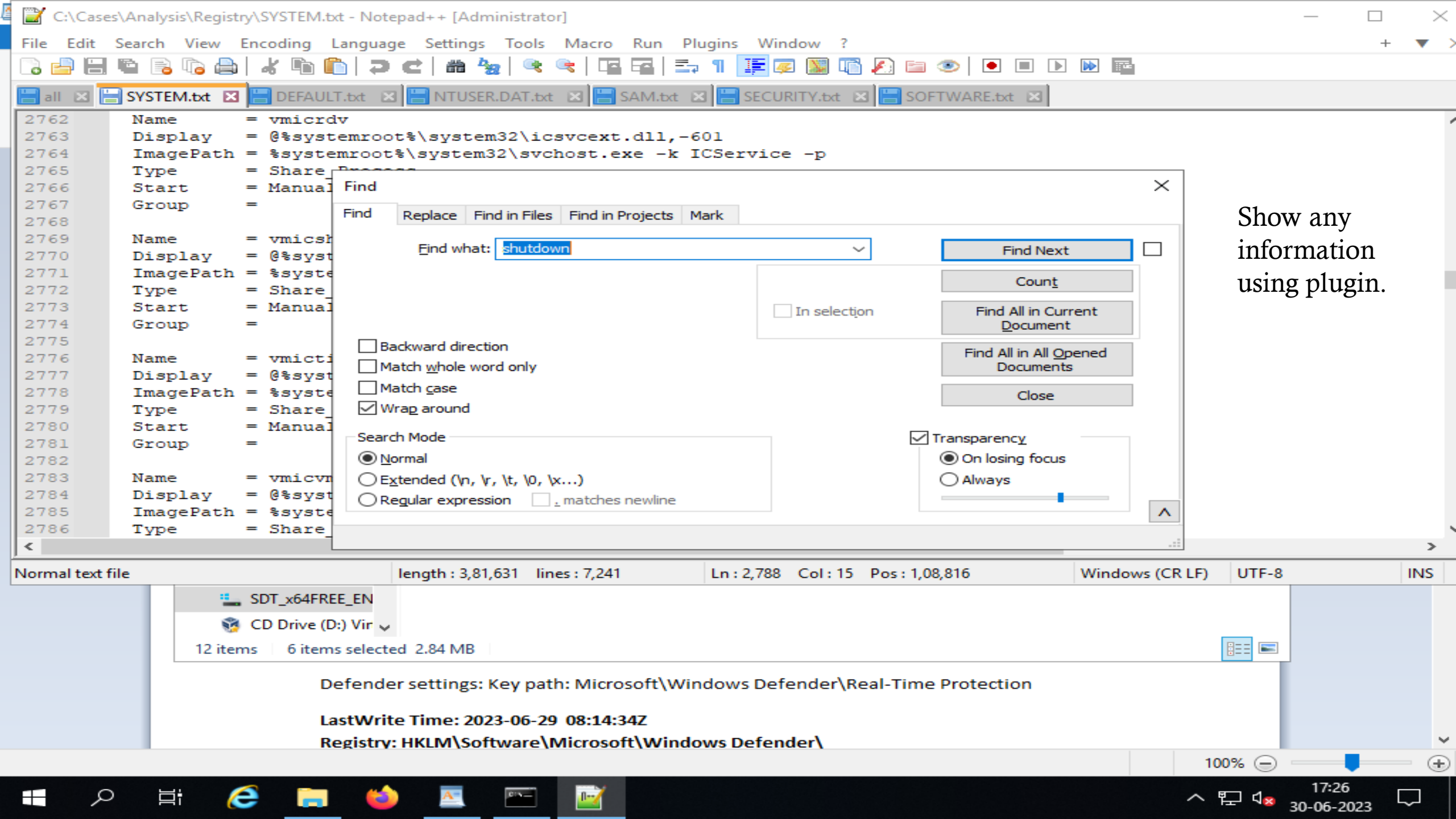
Execute the command for create the text file of registry hives.



Show the all text file of registry hives.



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



Show any information using plugin.

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 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

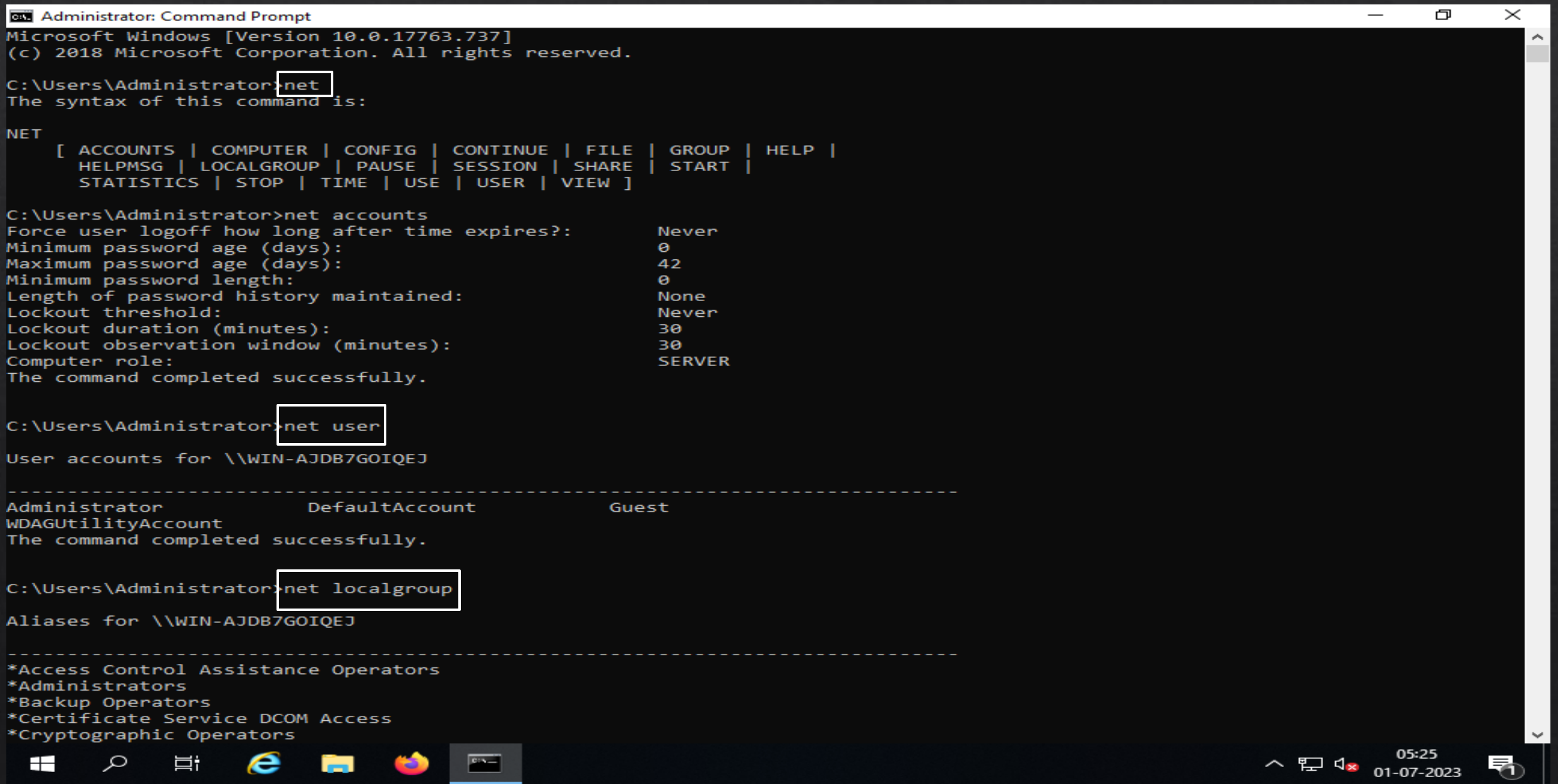
LastWrite Time: 2023-06-29 08:14:34Z

Registry: HKLM\Software\Microsoft\Windows Defender

100%

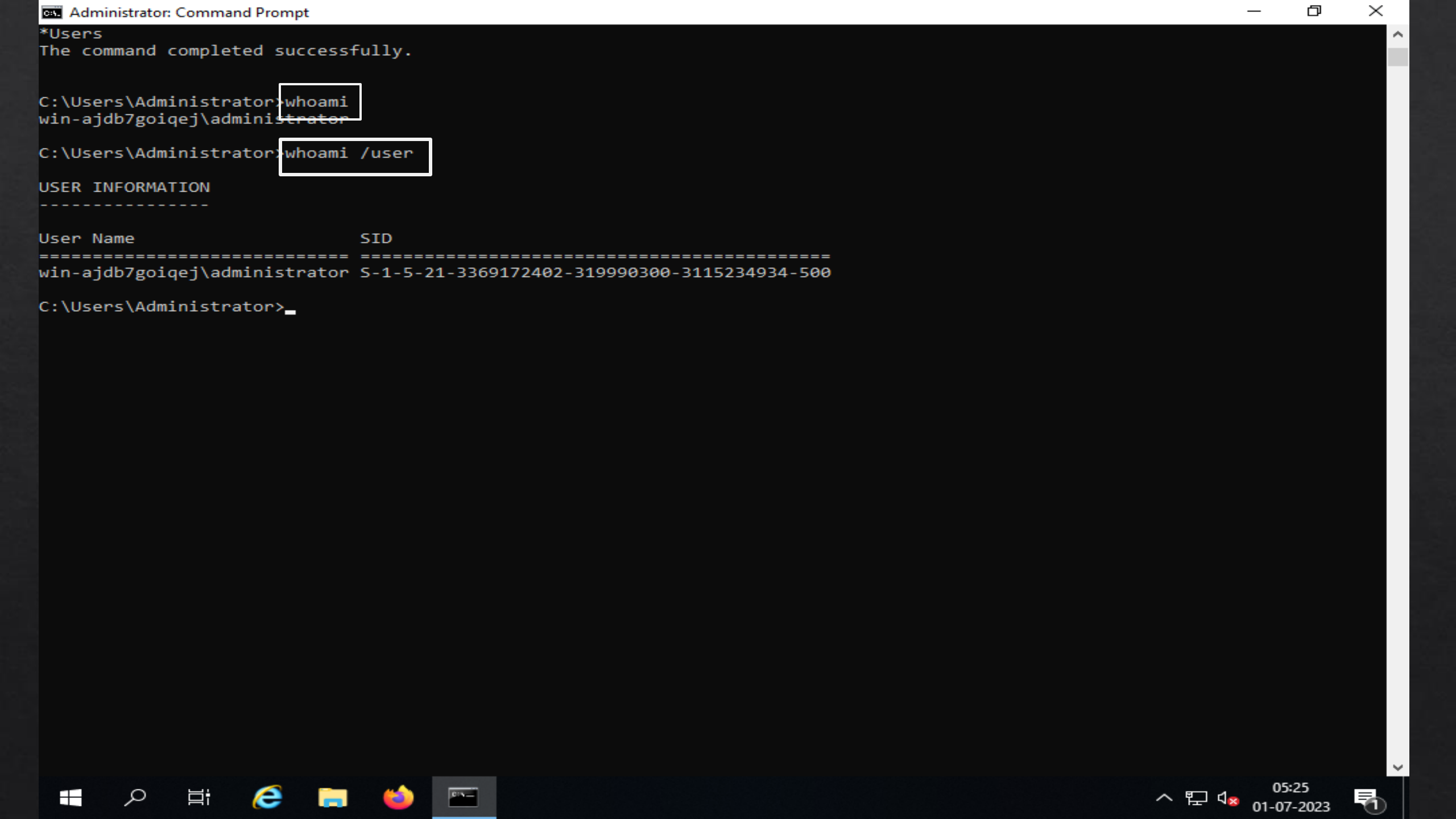
17:26
30-06-2023

User Accounts and SIDs Overview



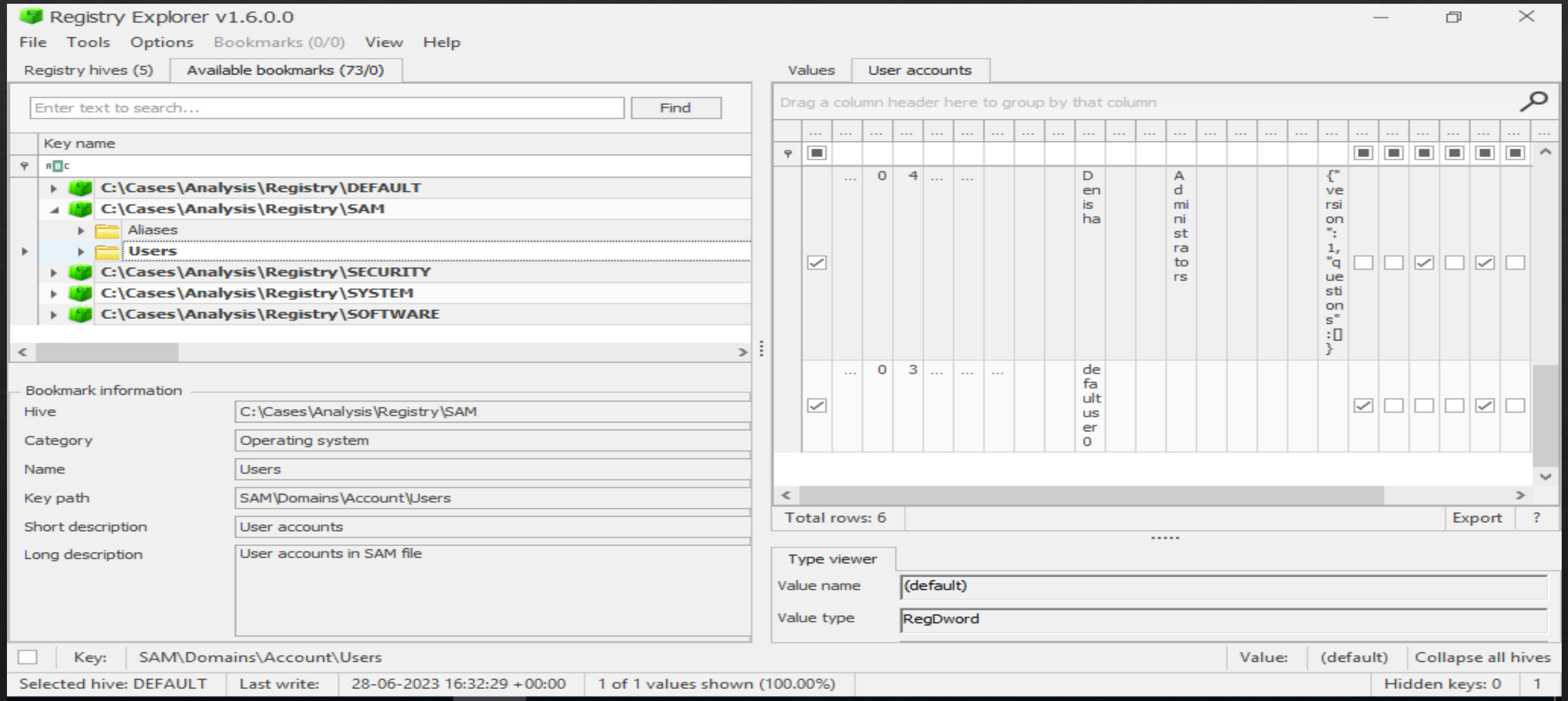
Administrator: Command Prompt

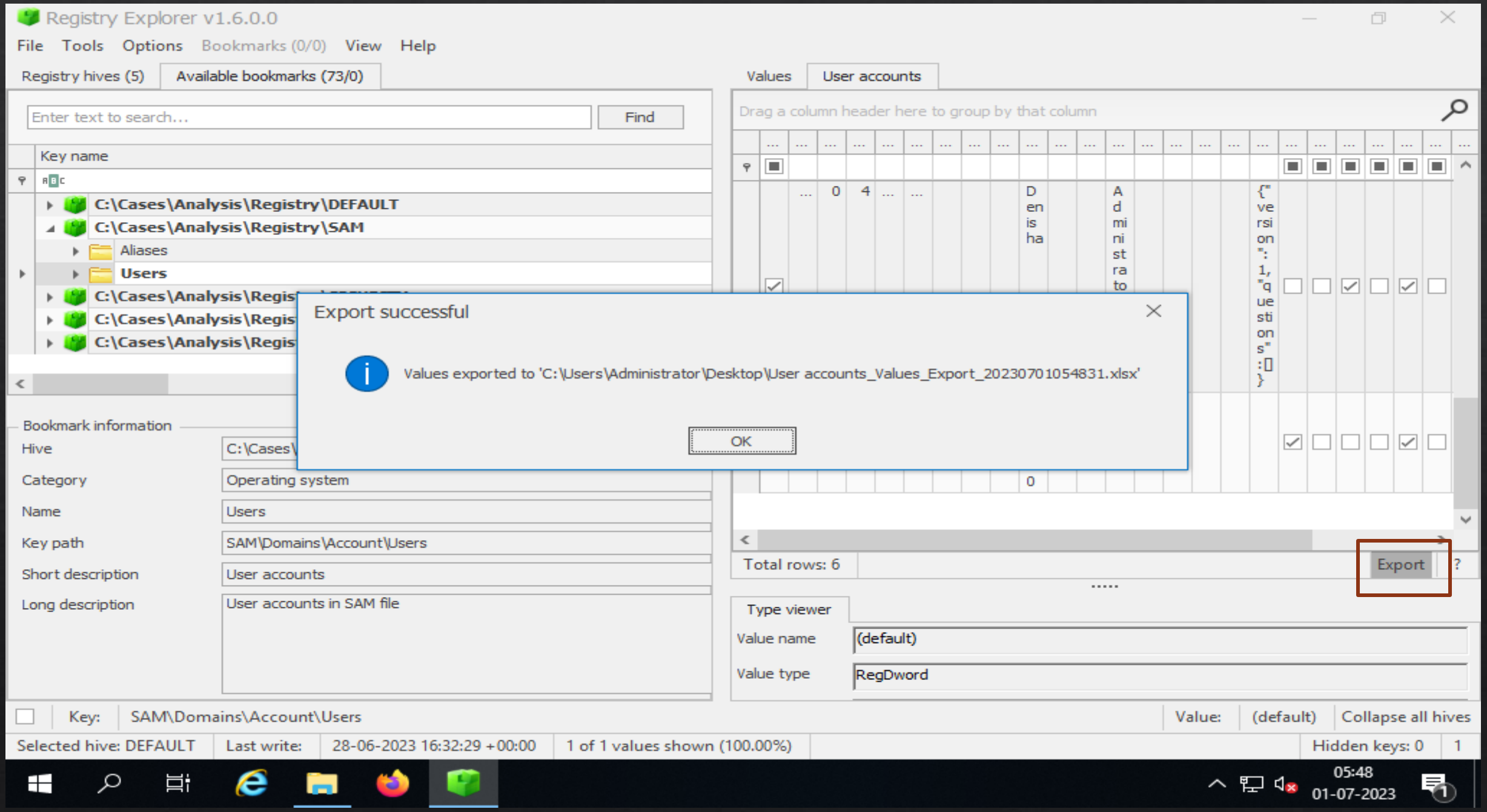
```
C:\Users\Administrator>net localgroup

Aliases for \\WIN-AJDB7GOIQEJ

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


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

C:\Users\Administrator>whoami /user

USER INFORMATION
----------------

User Name                     SID
============================= ============================================
```

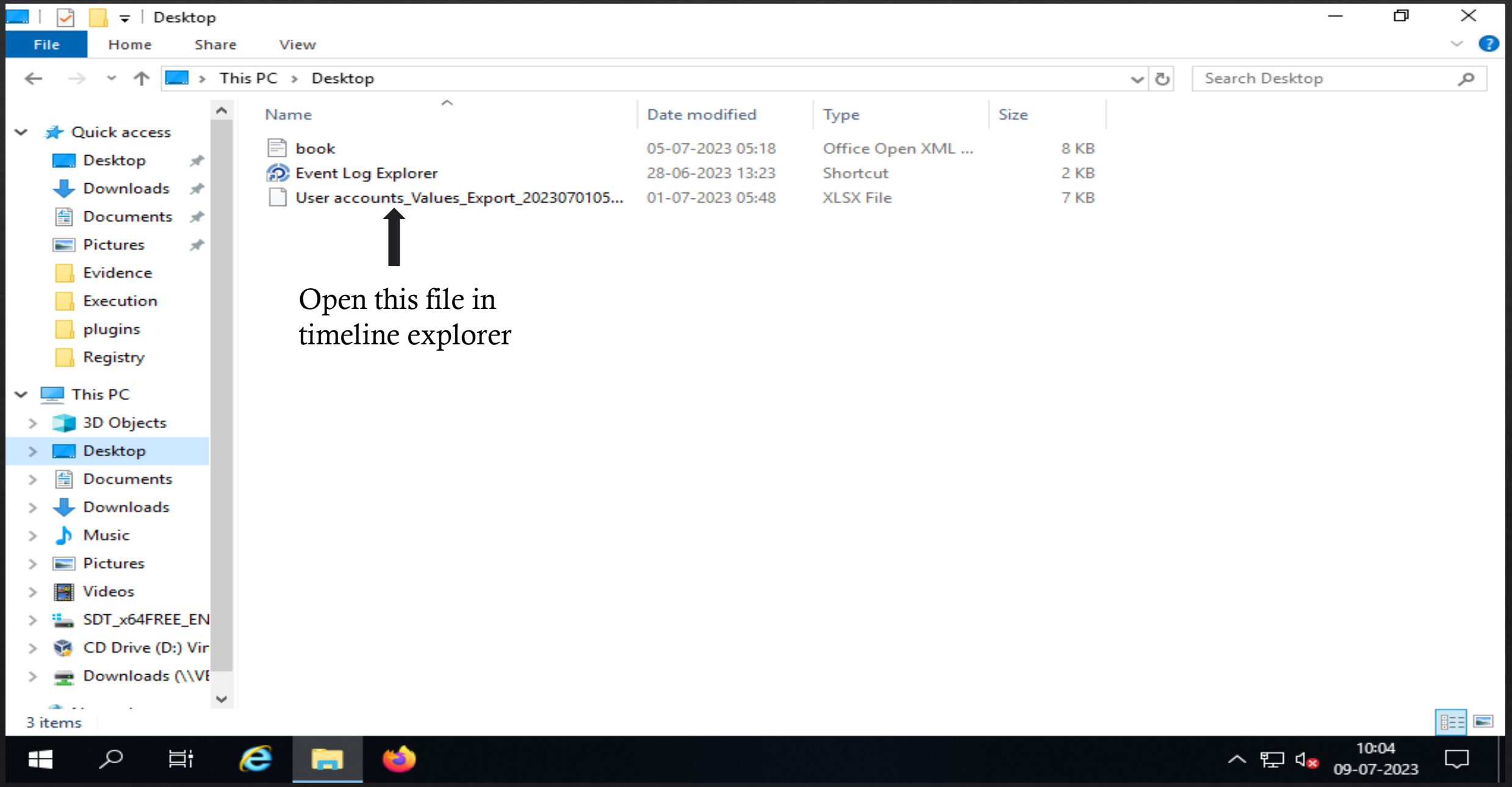

Administrator: Command Prompt
*Users
The command completed successfully.
C:\Users\Administrator>whoami
win-ajdb7goiqej\administrator
C:\Users\Administrator>whoami /user
USER INFORMATION
User Name SID
win-ajdb7goiqej\administrator S-1-5-21-3369172402-319990300-3115234934-500
C:\Users\Administrator>
05:25
01-07-2023

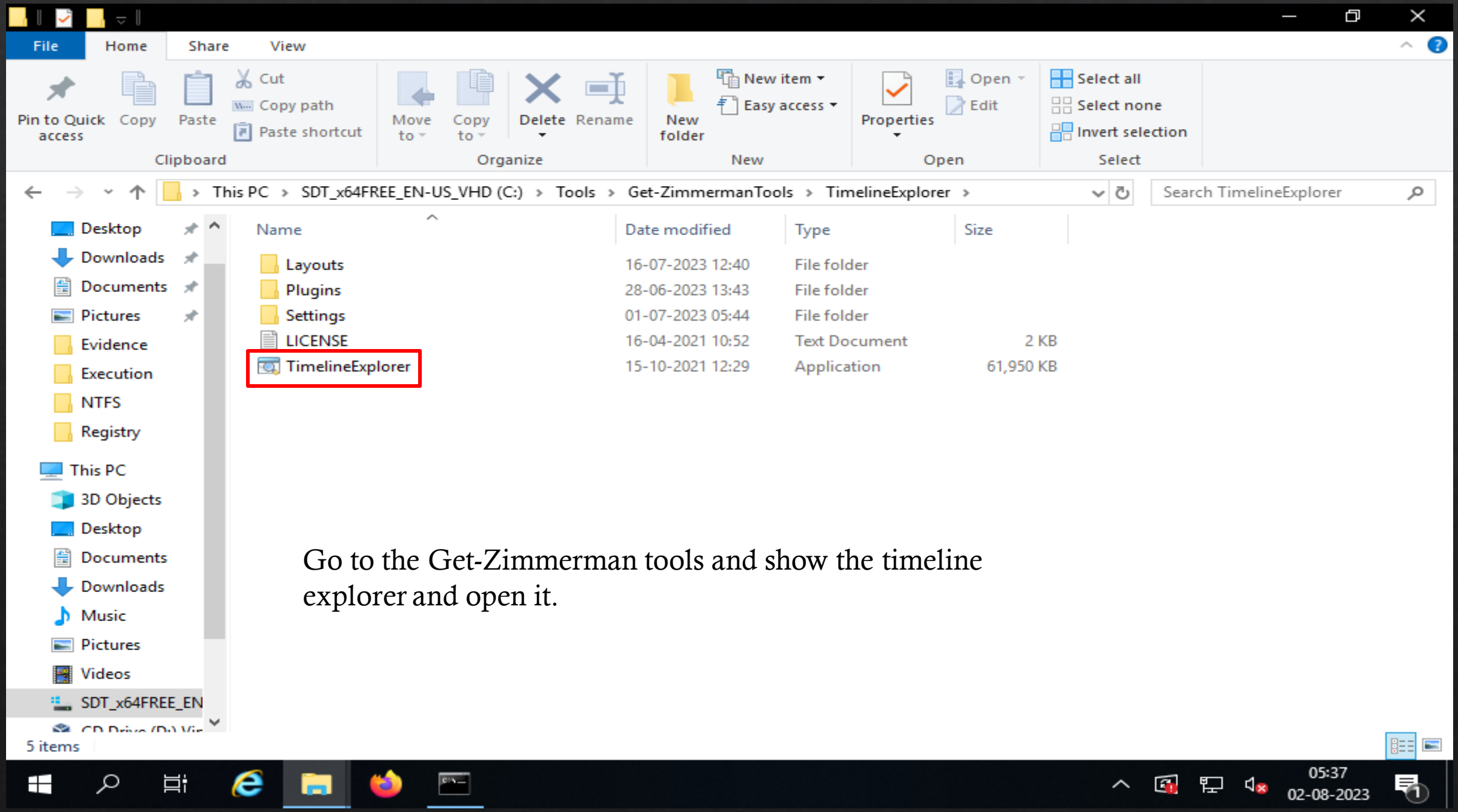
Analysis of user accounts , groups and profiles

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

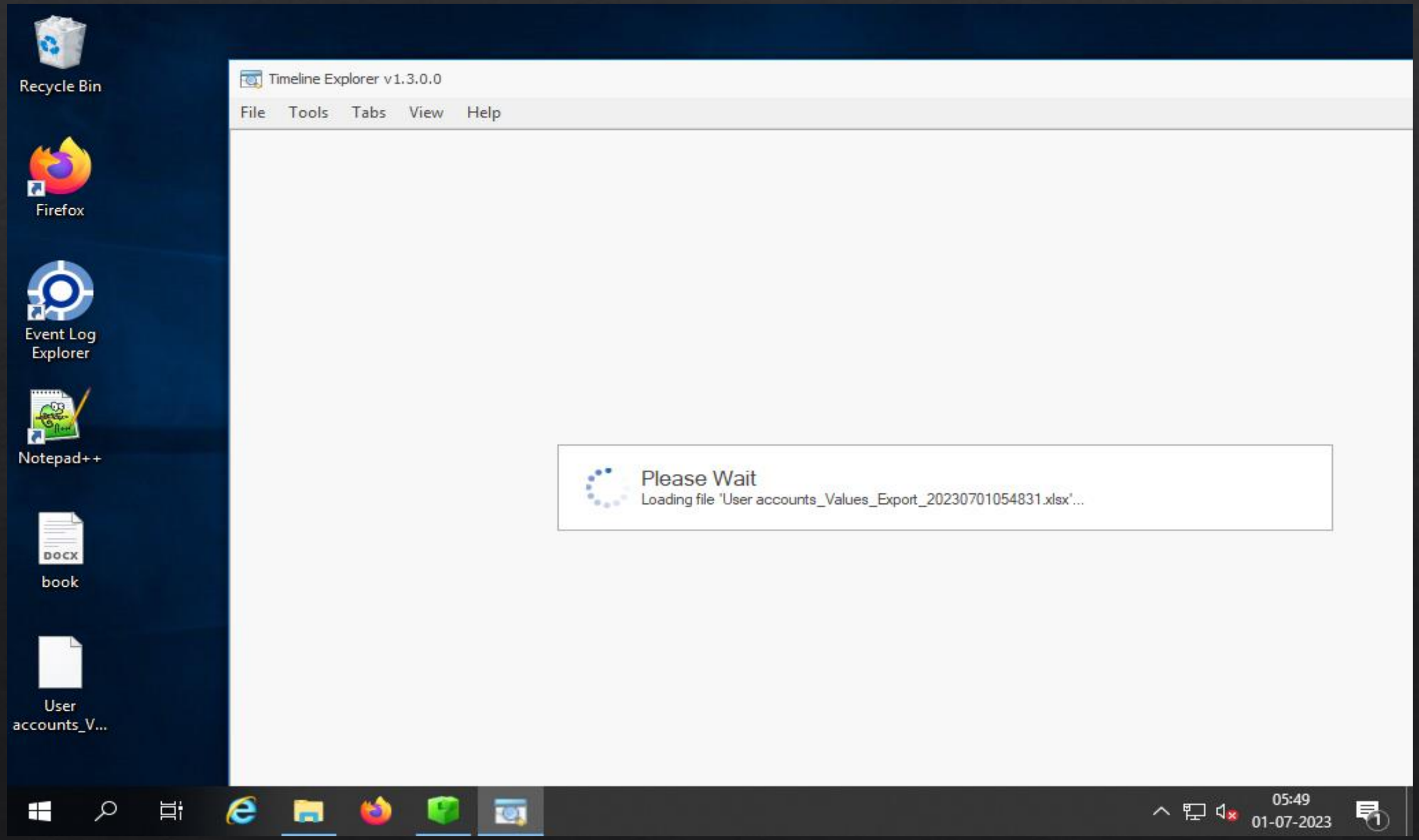


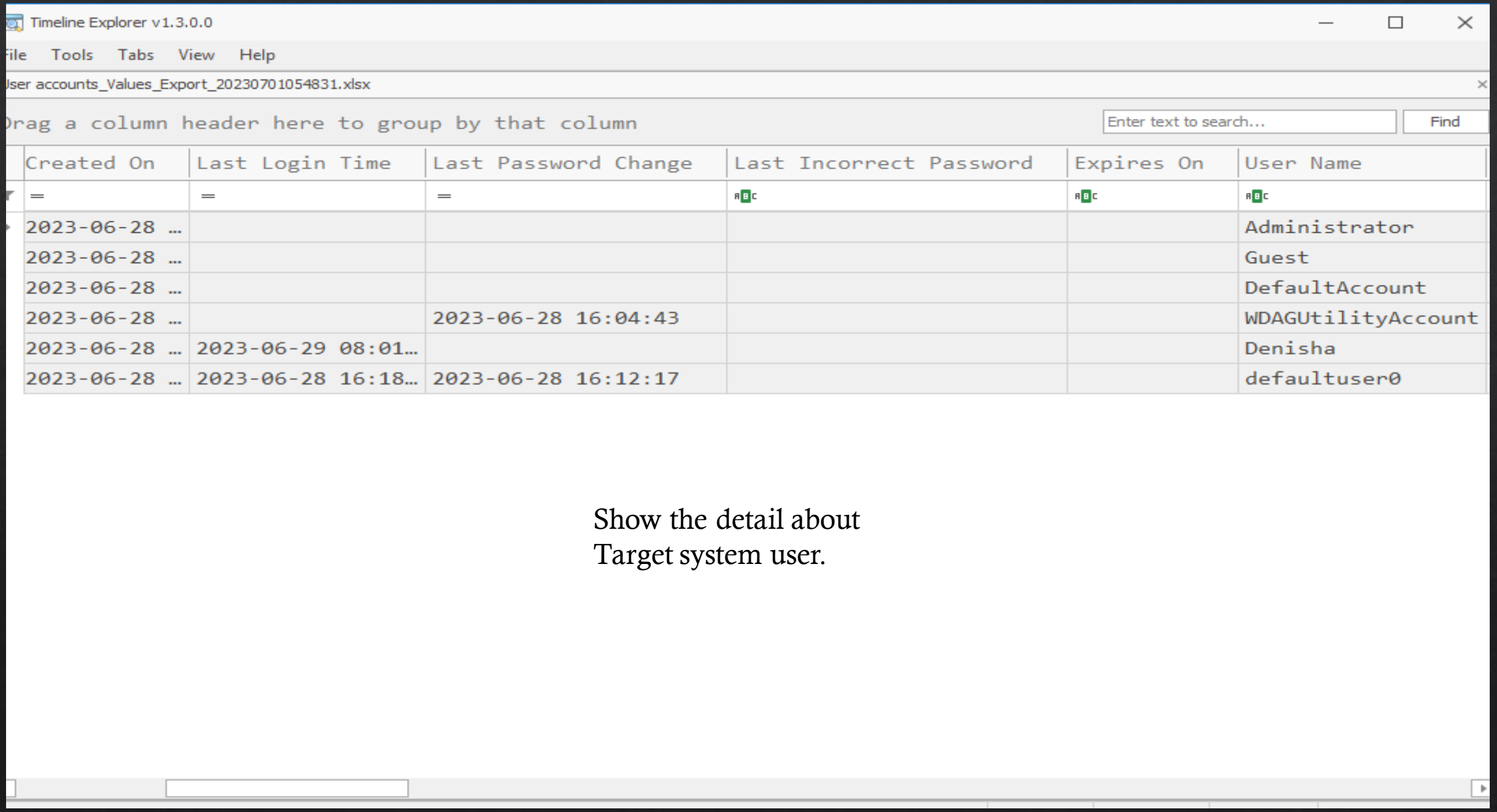

Registry Explorer v1.6.0.0
File Tools Options Bookmarks (0/0) View Help
Registry hives (5) Available bookmarks (73/0)
Enter text to search...
Find
Key name
C:\Cases\Analysis\Registry\DEFAULT
C:\Cases\Analysis\Registry\SAM
Aliases
Users
Values User accounts
Drag a column header here to group by that column
Export successful
Values exported to 'C:\Users\Administrator\Desktop\User accounts_Values_Export_20230701054831.xlsx'
OK
Bookmark information
Hive
Category Operating system
Name Users
Key path SAM\Domains\Account\Users
Short description User accounts
Long description User accounts in SAM file
Total rows: 6
Export
Type viewer
Value name (default)
Value type RegDword
Key: SAM\Domains\Account\Users
Value: (default)
Collapse 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
05:48
01-07-2023


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 (\\VE
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
3 items
10:04
09-07-2023

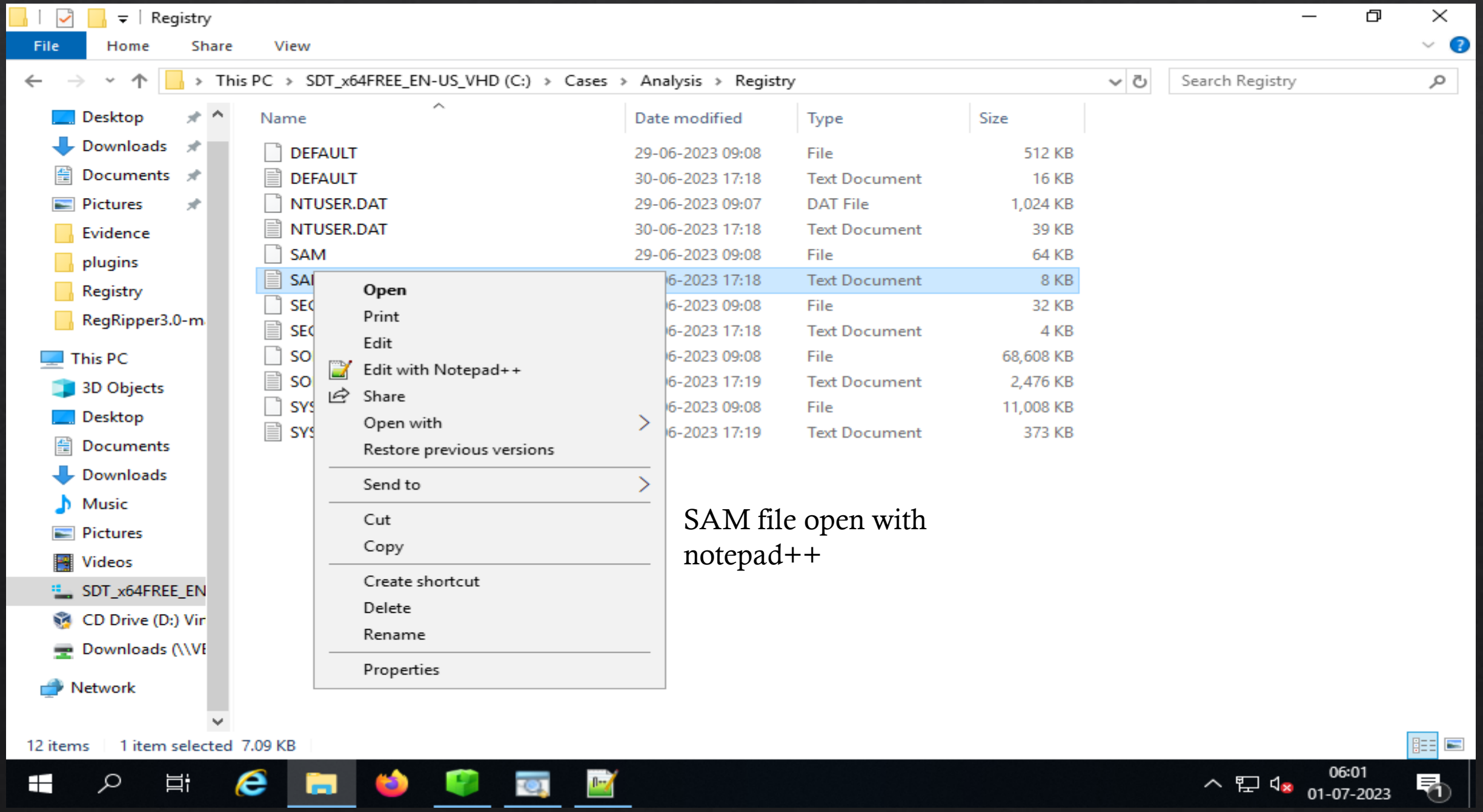


Go to the Get-Zimmerman tools and show the timeline explorer and open it.


Recycle Bin
Firefox
Event Log Explorer
Notepad++
book
User accounts_V...
Timeline Explorer v1.3.0.0
File
Tools
Tabs
View
Help
Please Wait
Loading file 'User accounts_Values_Export_20230701054831.xlsx'...
05:49
01-07-2023



Show the detail about
Target system user.



SAM file open with notepad++

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

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

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

```
samparse v.20220921
(SAM) Parse SAM file for user & group mbrshp info


User Information
------------------------
Username        : Administrator [500]
SID             : S-1-5-21-3331464962-214784631-3394824829-500
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    :
Account Created : Wed Jun 28 16:13:16 2023 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Account Disabled
  --> Normal user account

Username        : Guest [501]
SID             : S-1-5-21-3331464962-214784631-3394824829-501
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    :
Account Created : Wed Jun 28 16:13:16 2023 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
```

Show the user detail using Notepad++.

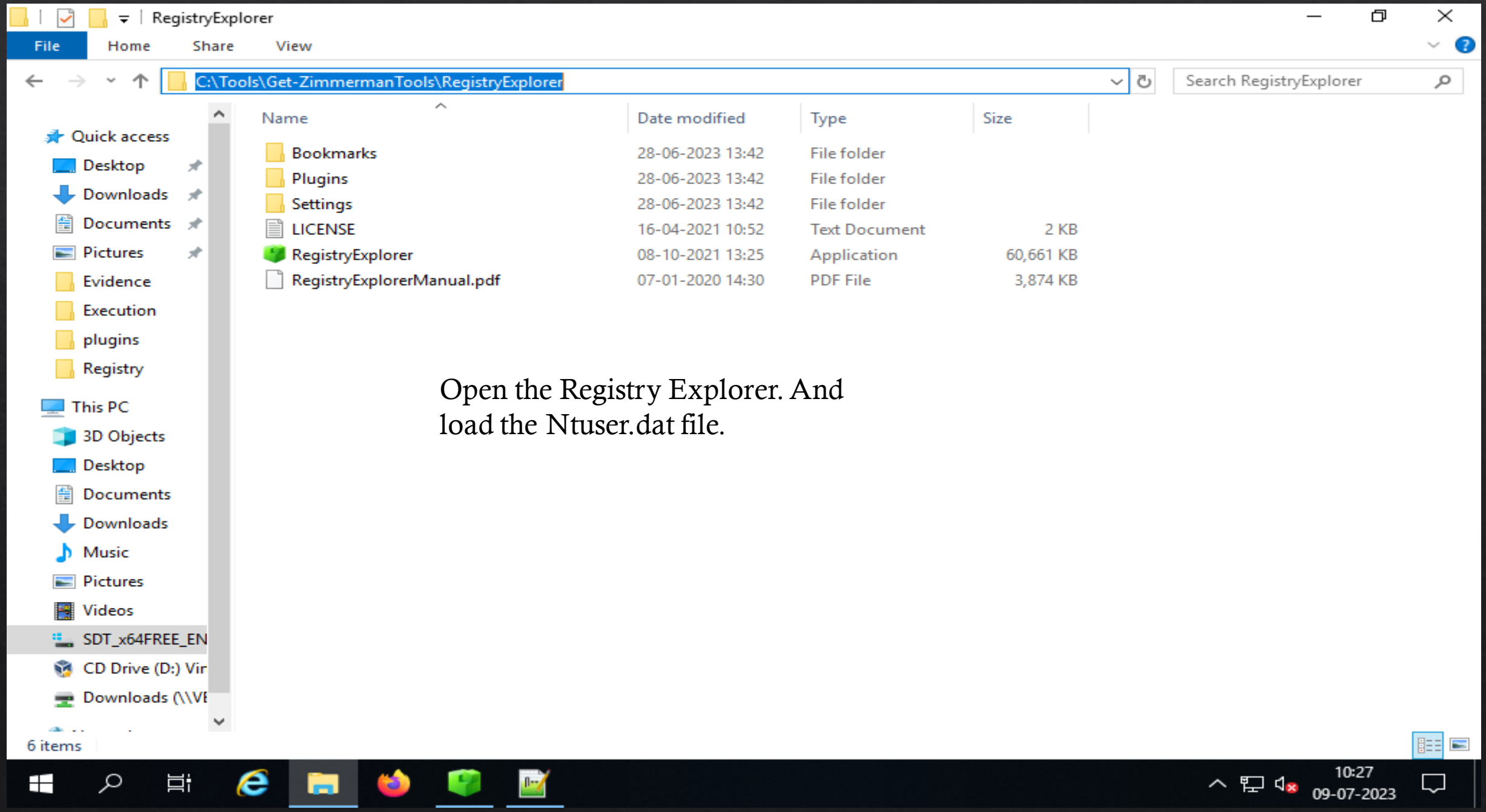
Normal text file | length : 7,269 | lines : 202 | Ln : 20 | Col : 26 | Pos : 583 | Windows (CR LF) | UTF-8 | INS

06:01
01-07-2023

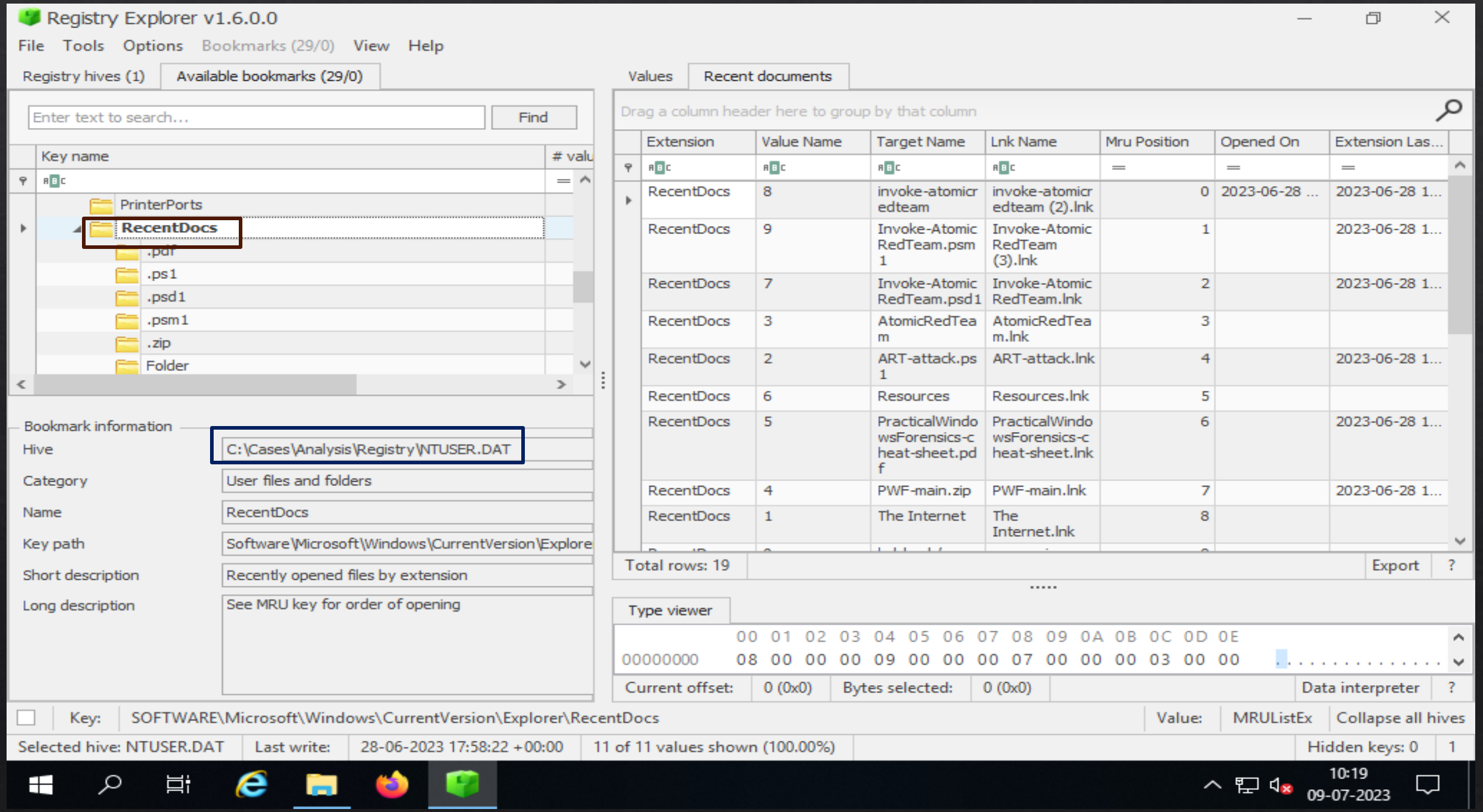
RecentDocs Analysis

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

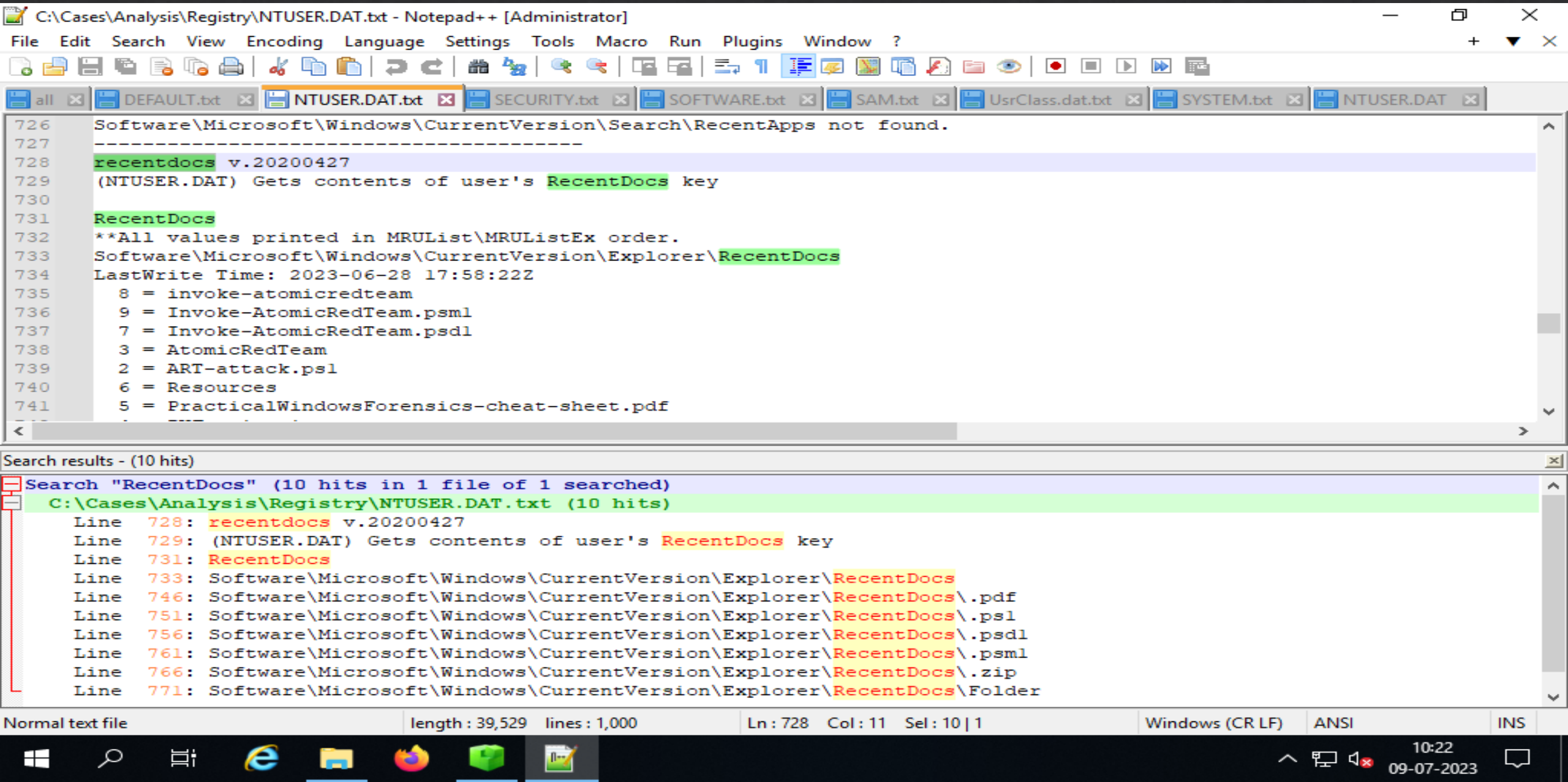
Load the Ntuser.dat hive on Registry Explorer. And open Recent Doc.



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


Registry Explorer v1.6.0.0
File Tools Options Bookmarks (29/0) View Help
Registry hives (1) Available bookmarks (29/0)
Enter text to search...
Find
Key name
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\Explore
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...
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

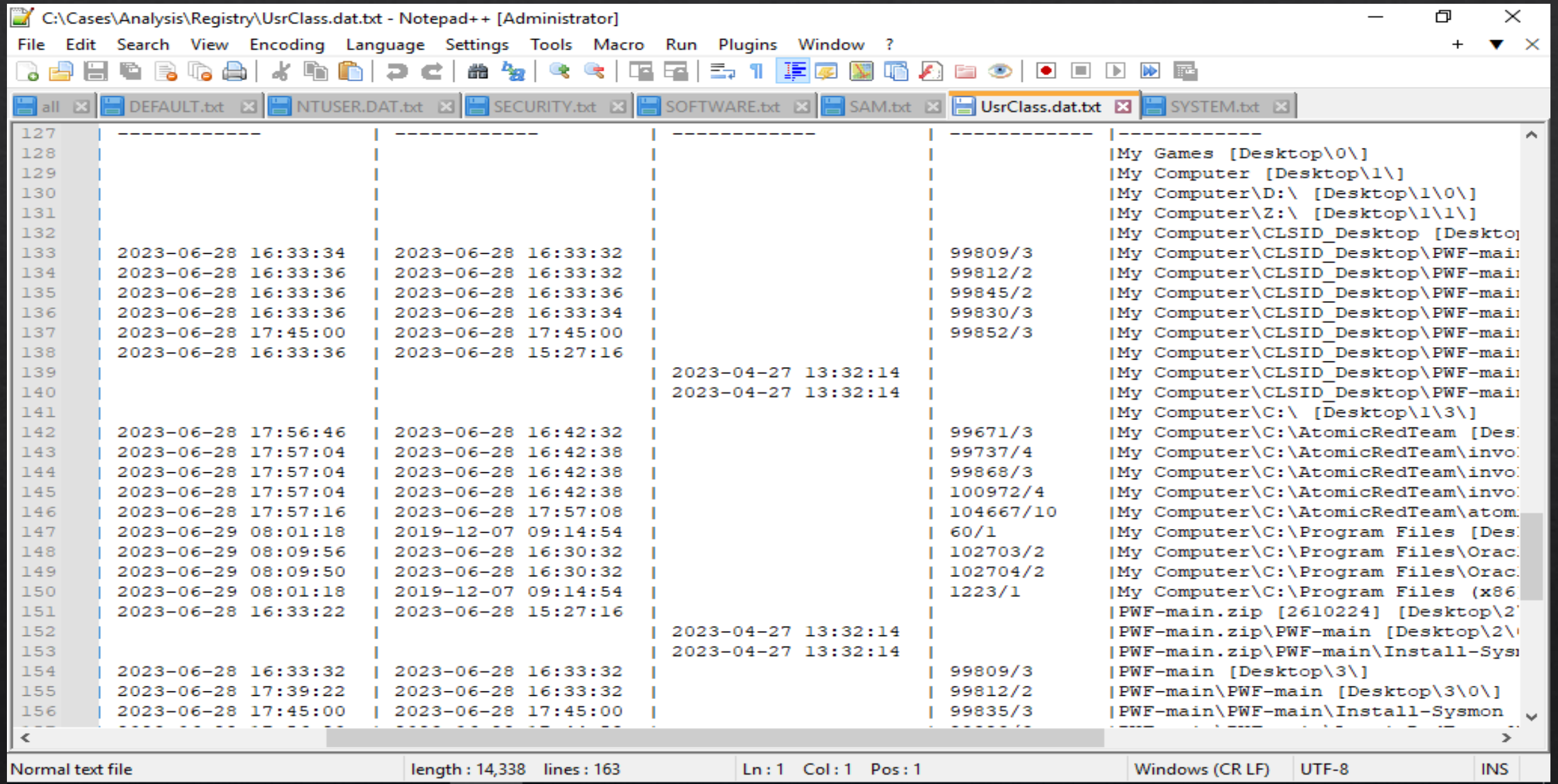
Open Ntuser.dat file in Notepad++.



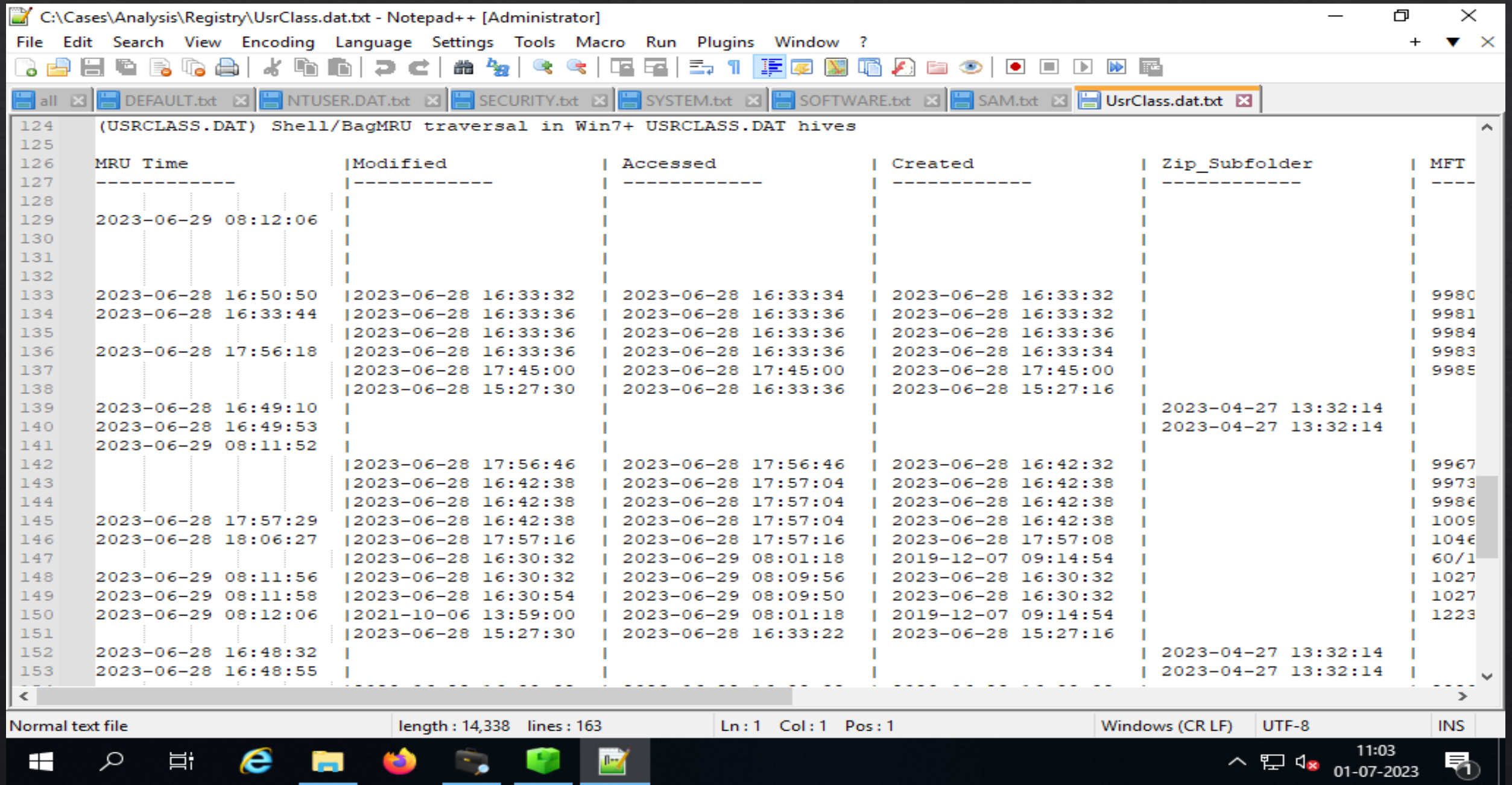
ShellBags Analysis

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.

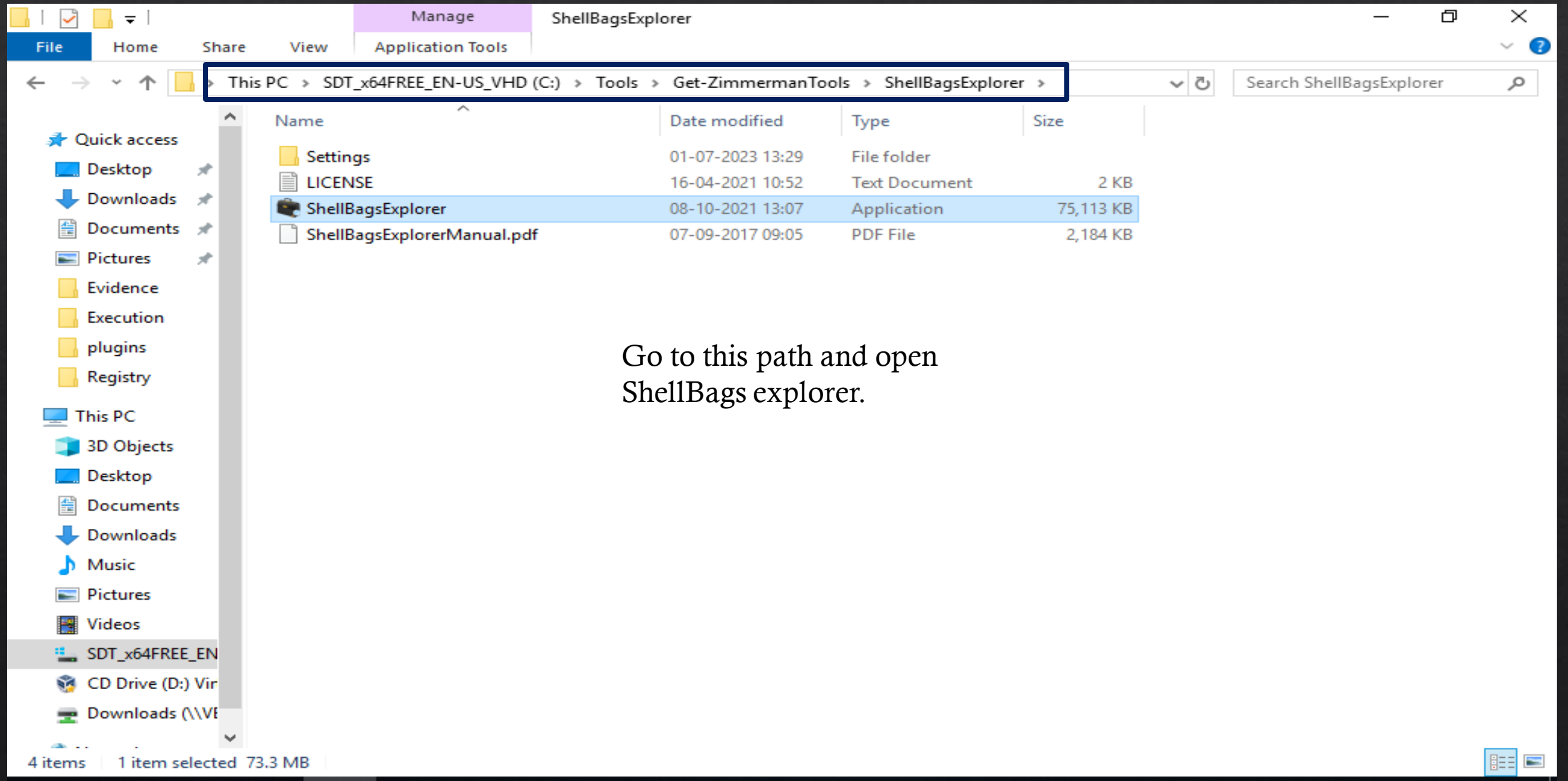
Usrclass.txt file edit with Notepad++.



Usrclass.txt file edit with Notepad++.

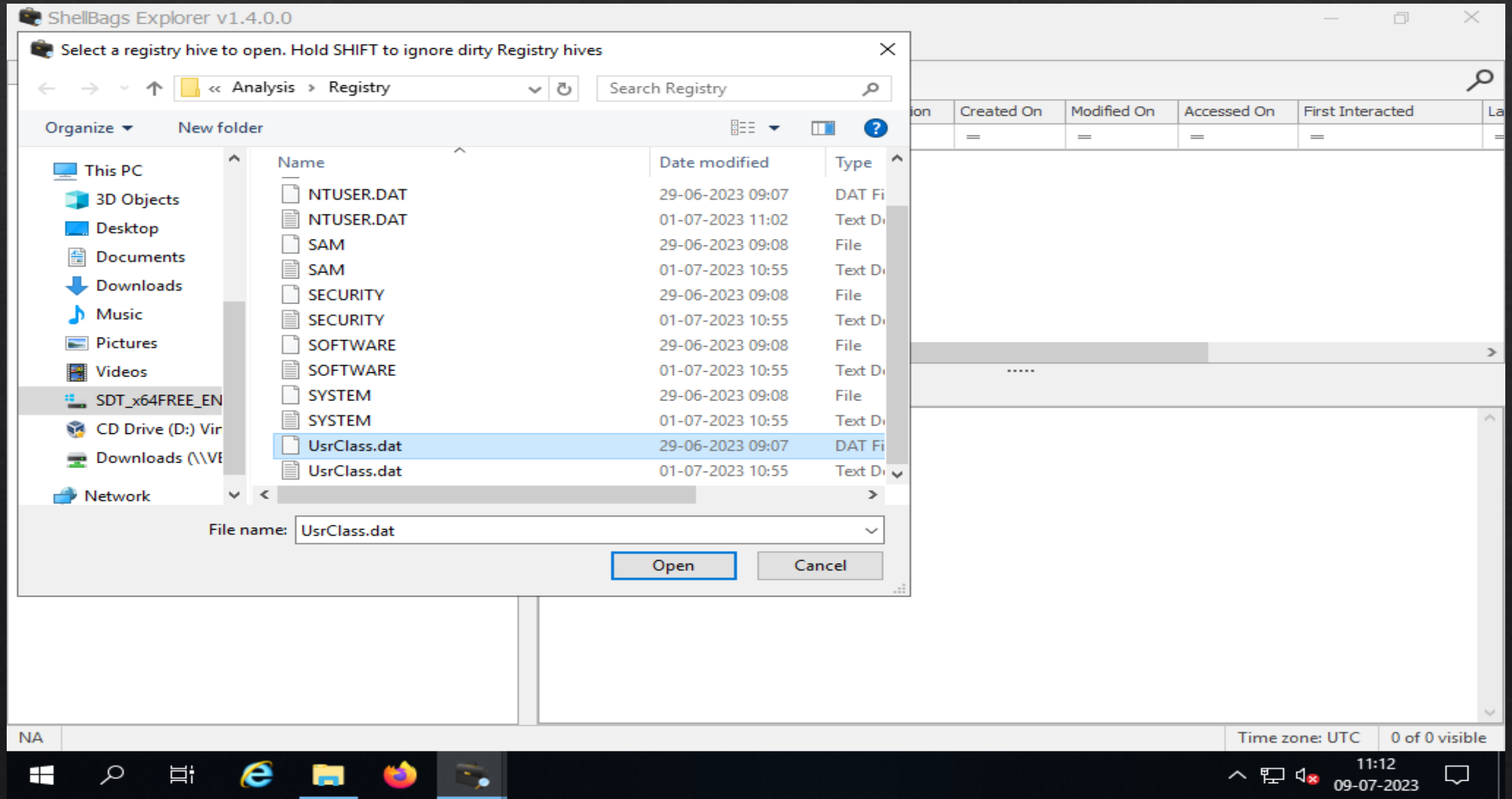


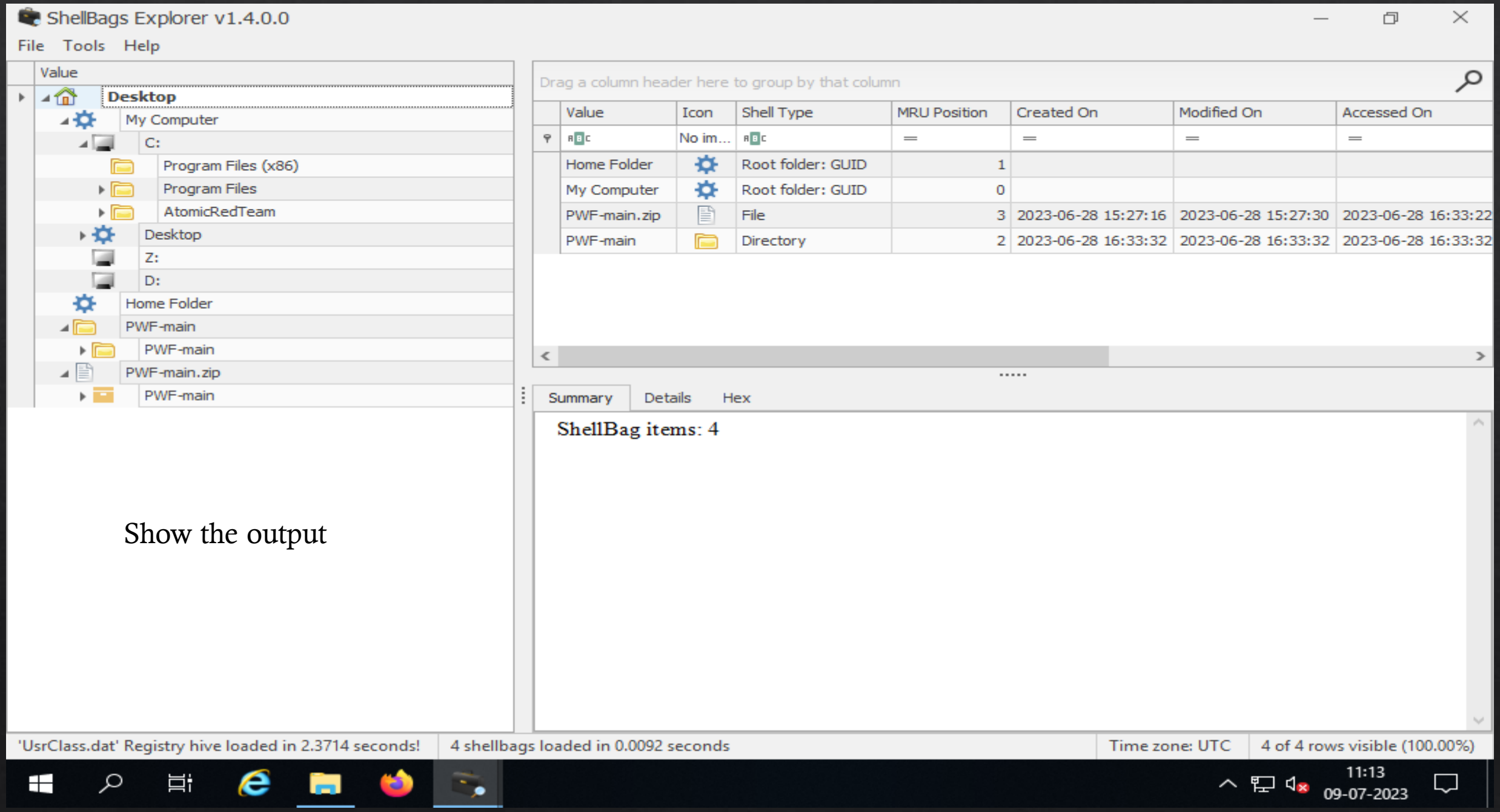
Open the ShellBagsExplorer



Go to this path and open ShellBags explorer.

Insert the UsrClass.dat

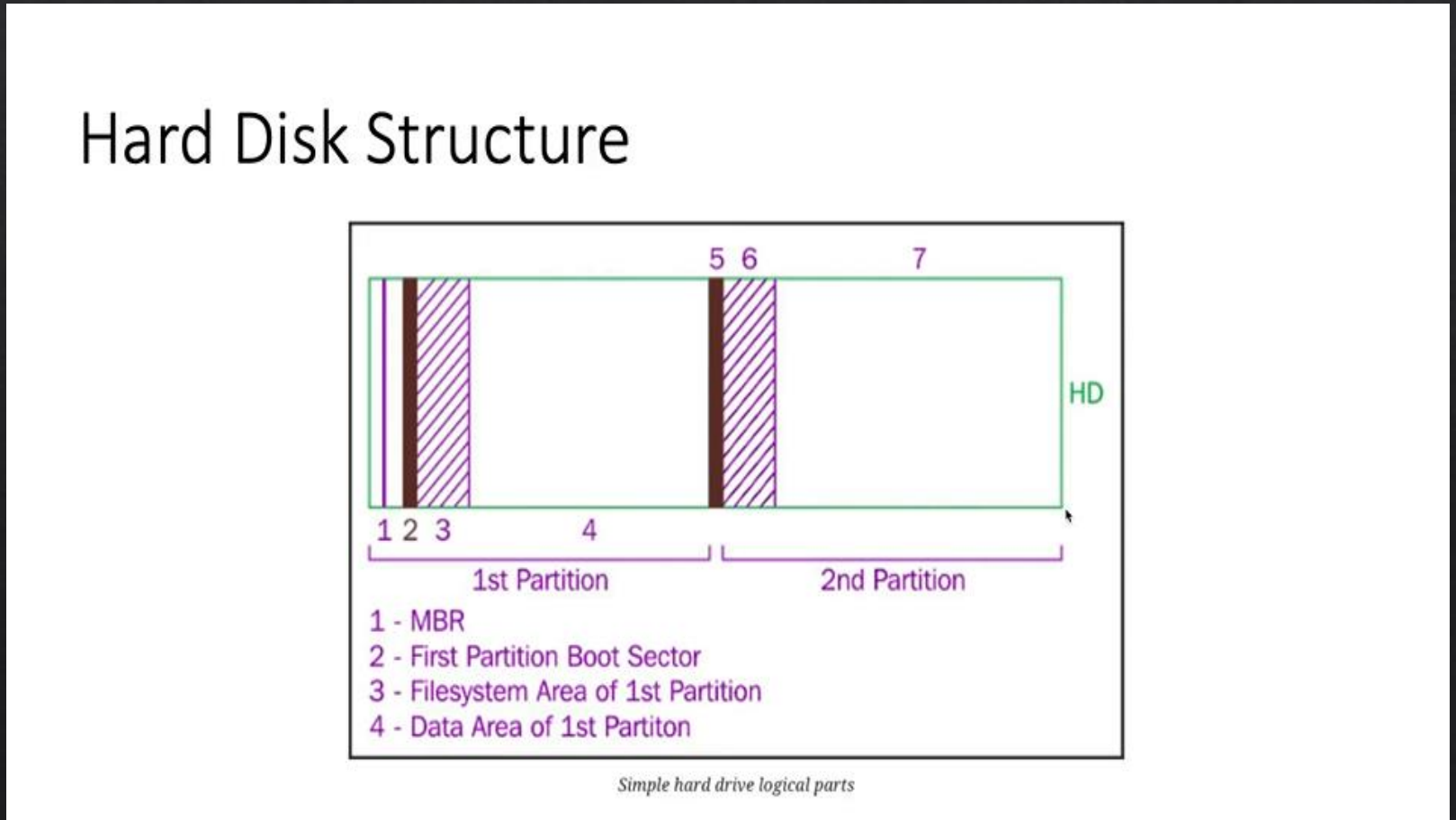




Show the output

NTFS- File system Analysis

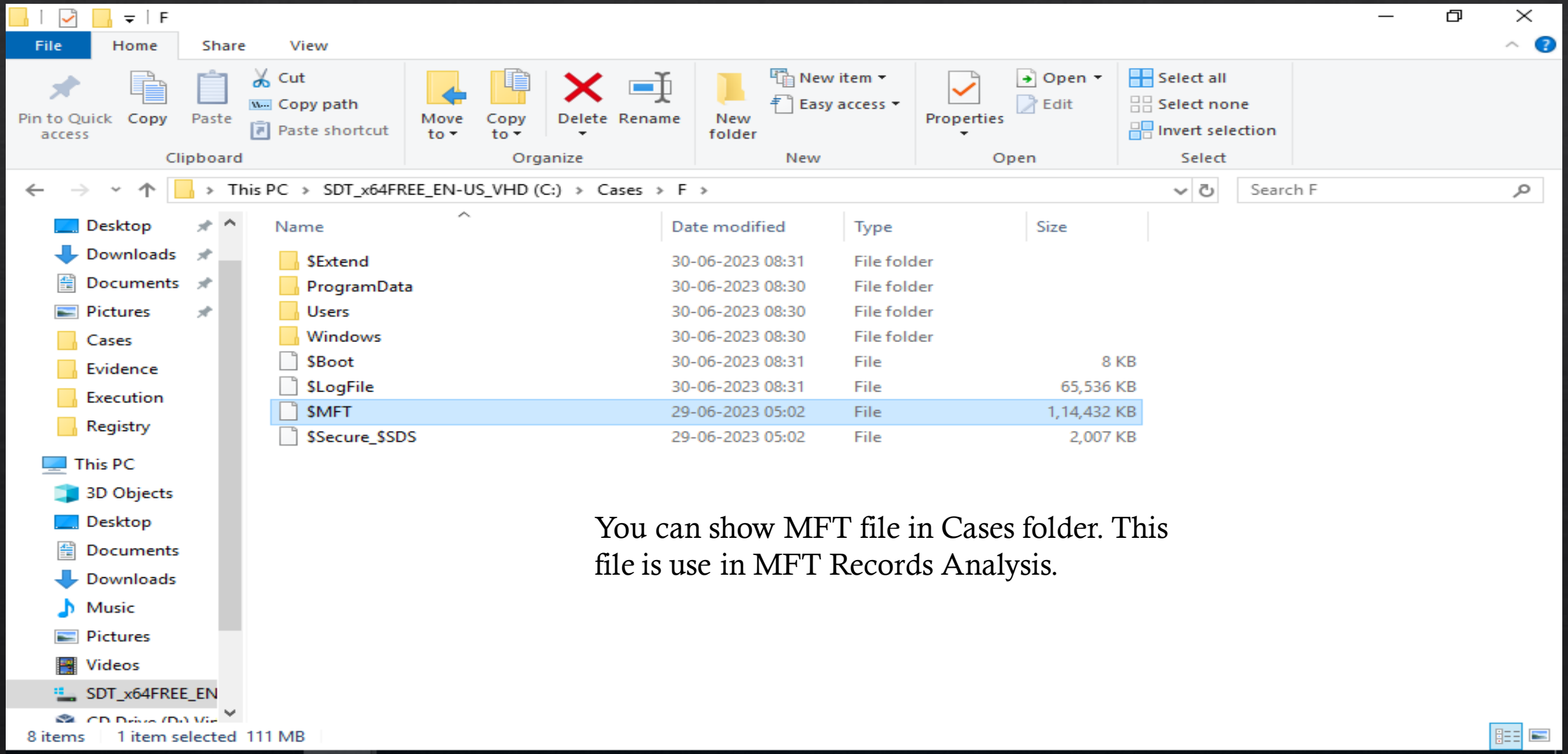
NT file system (NTFS), which is also sometimes called the New Technology File System, is a process that the Windows NT operating system uses for storing, organizing, and finding files on a hard disk efficiently



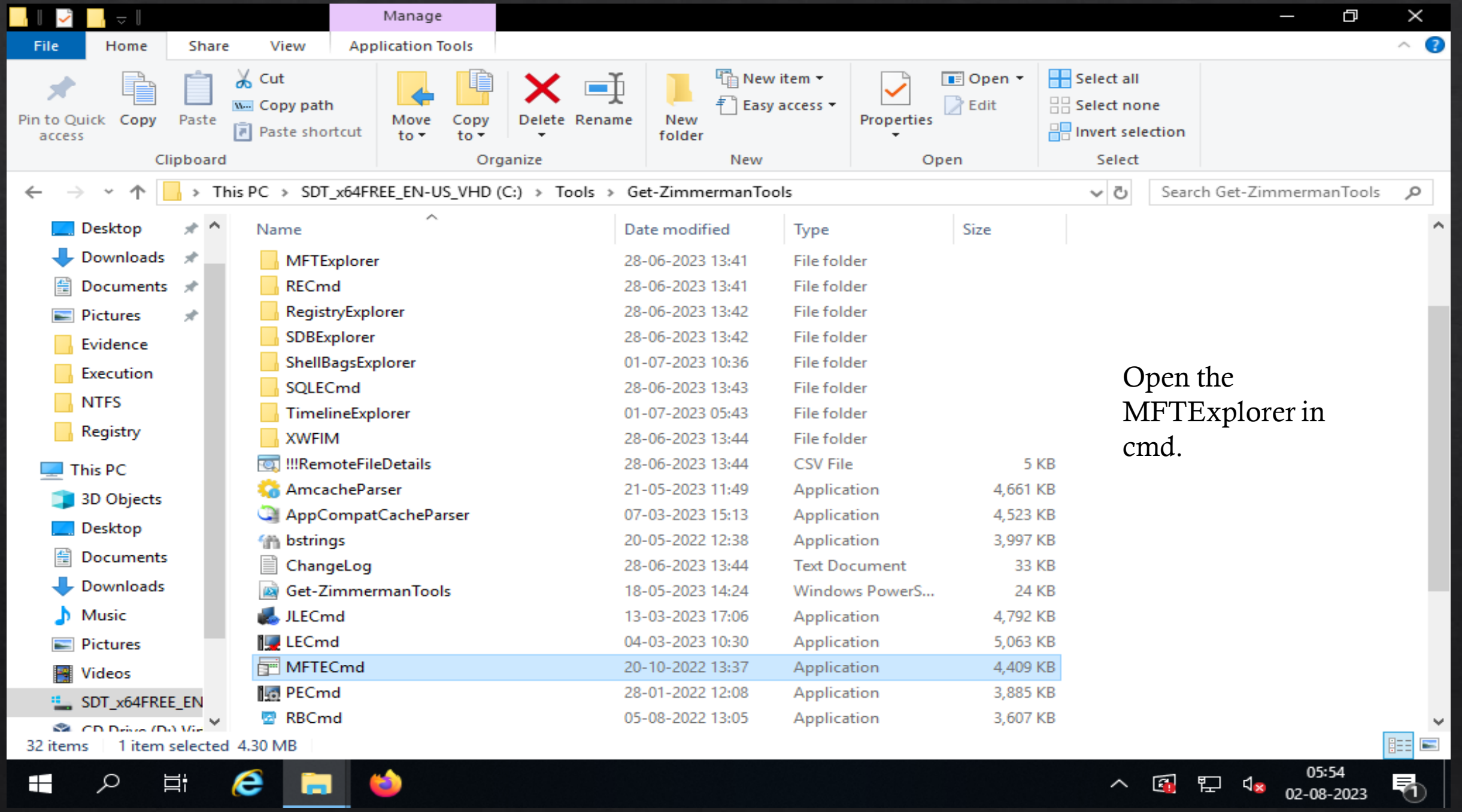
MFT(Master File Table) records

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



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

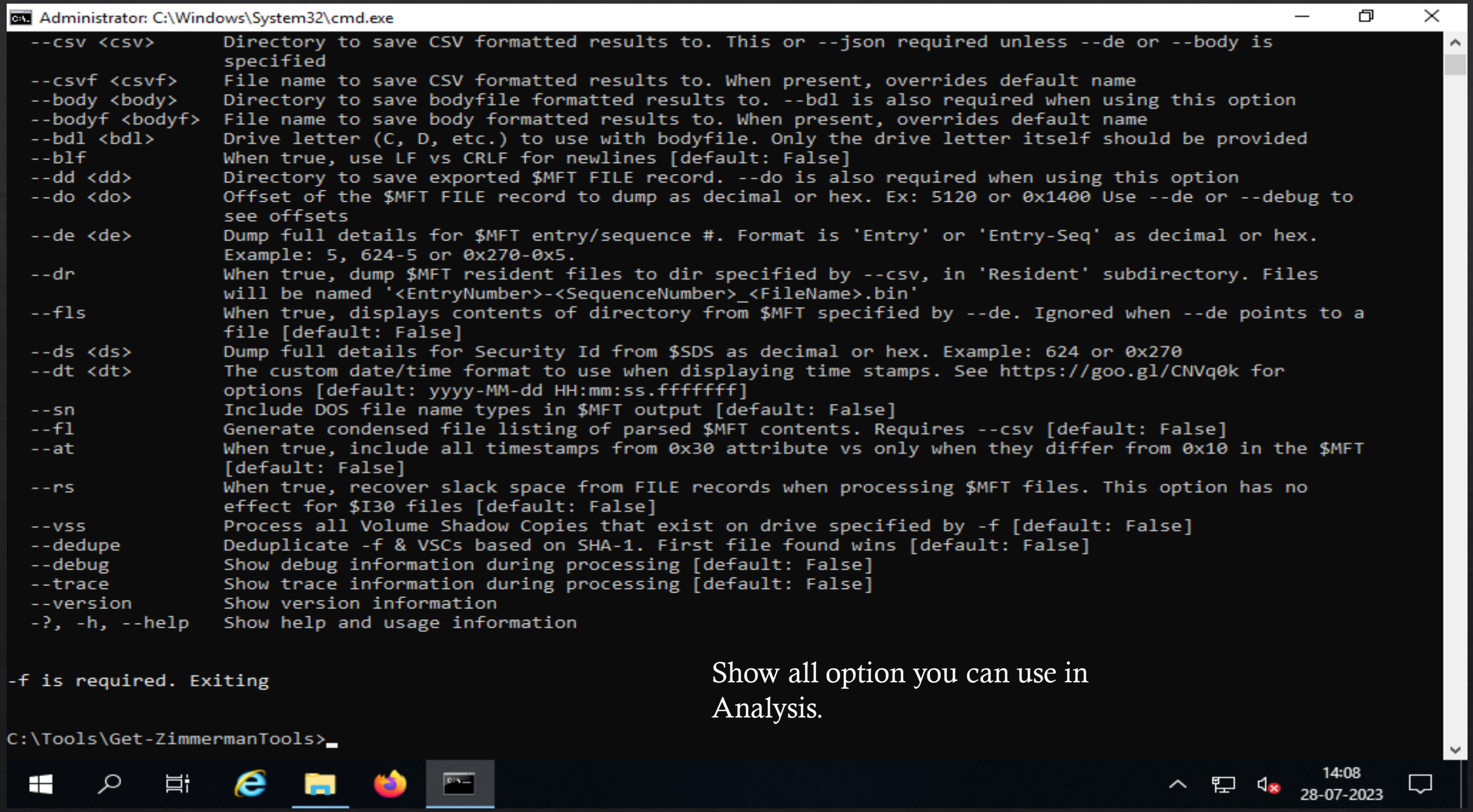


Open the MFTExplorer in cmd.

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

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

C:\Tools\Get-ZimmermanTools>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

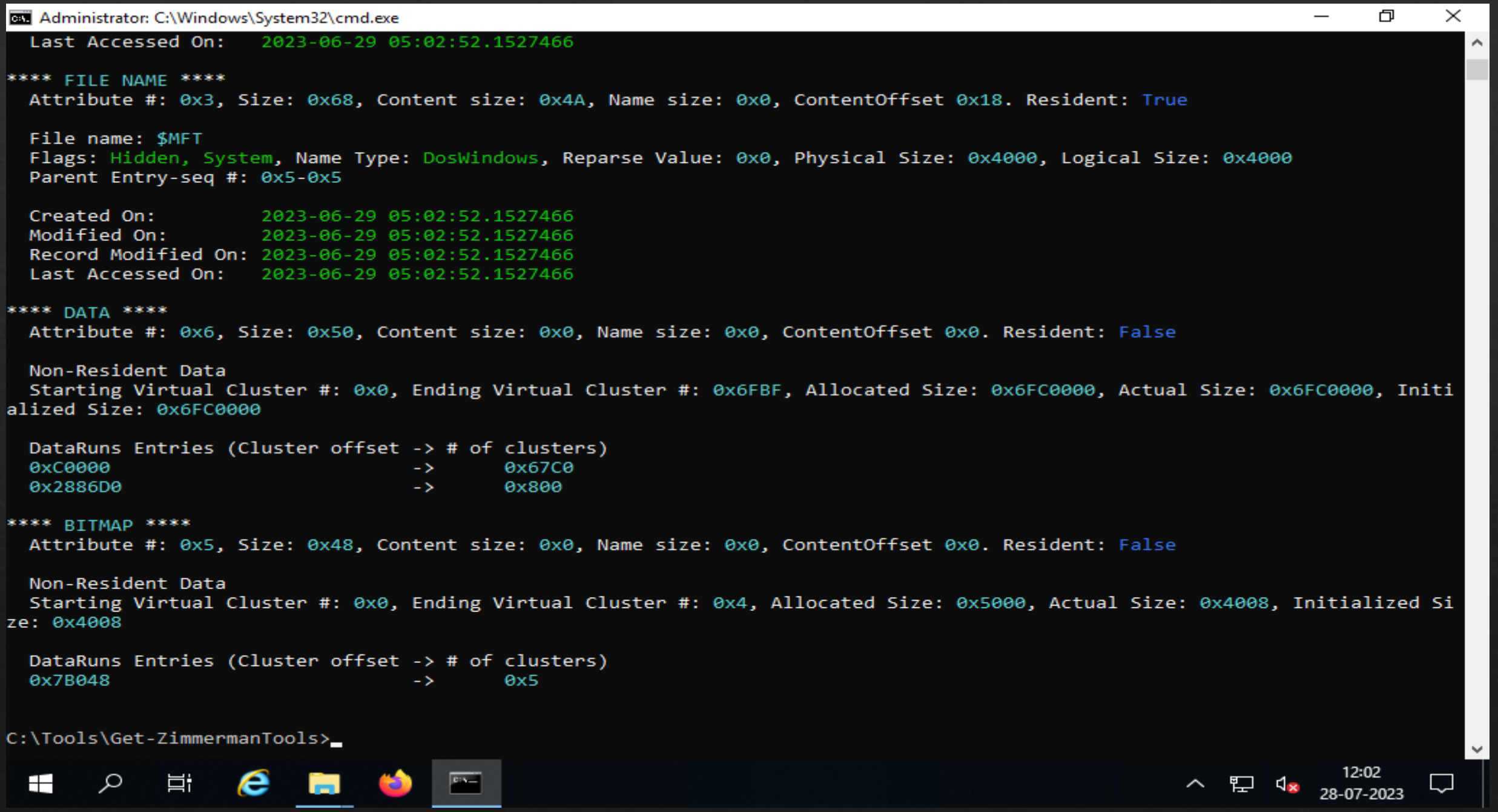


Show all option you can use in Analysis.

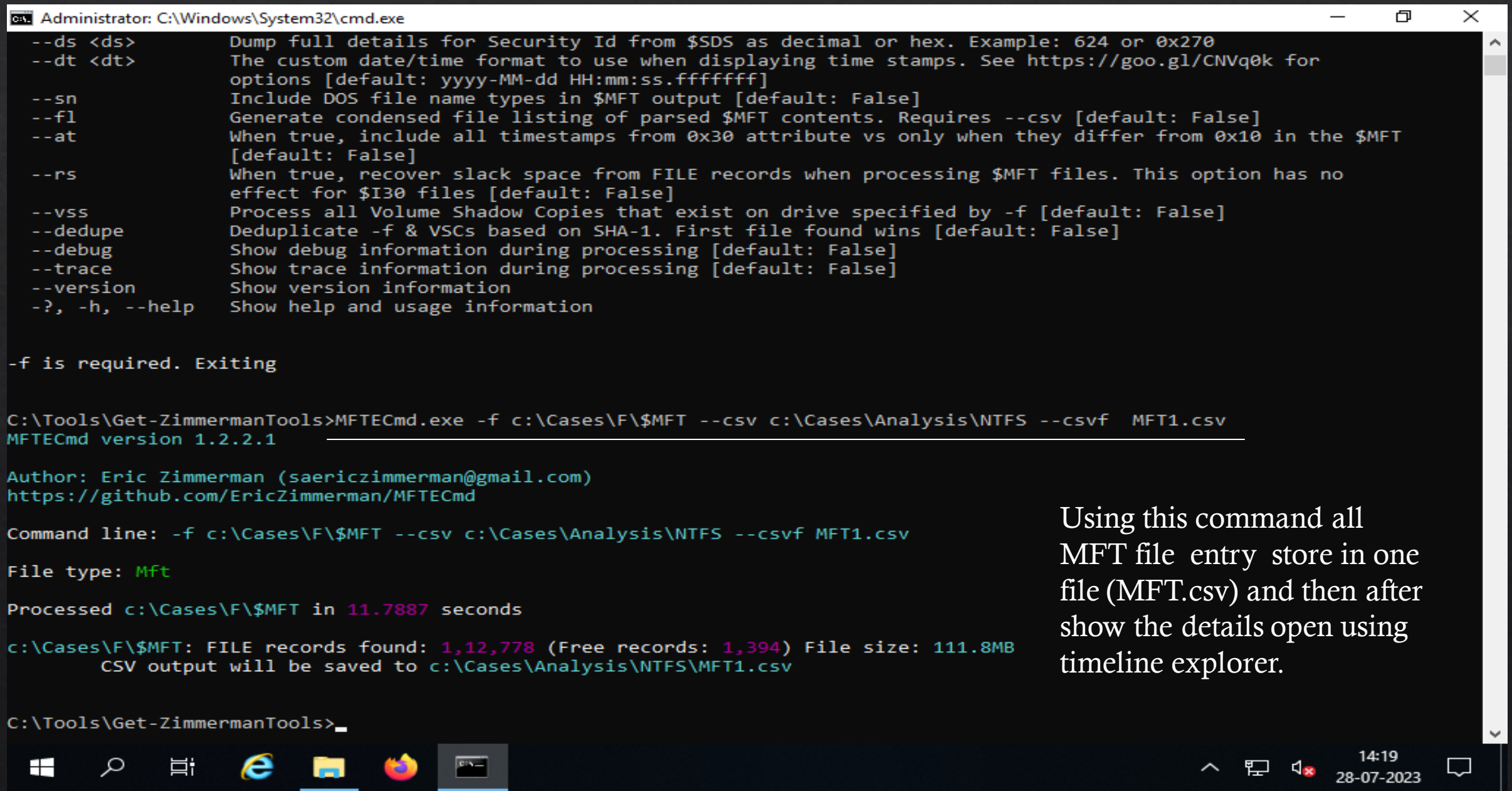
Administrator: C:\Windows\System32\cmd.exe

```
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
```

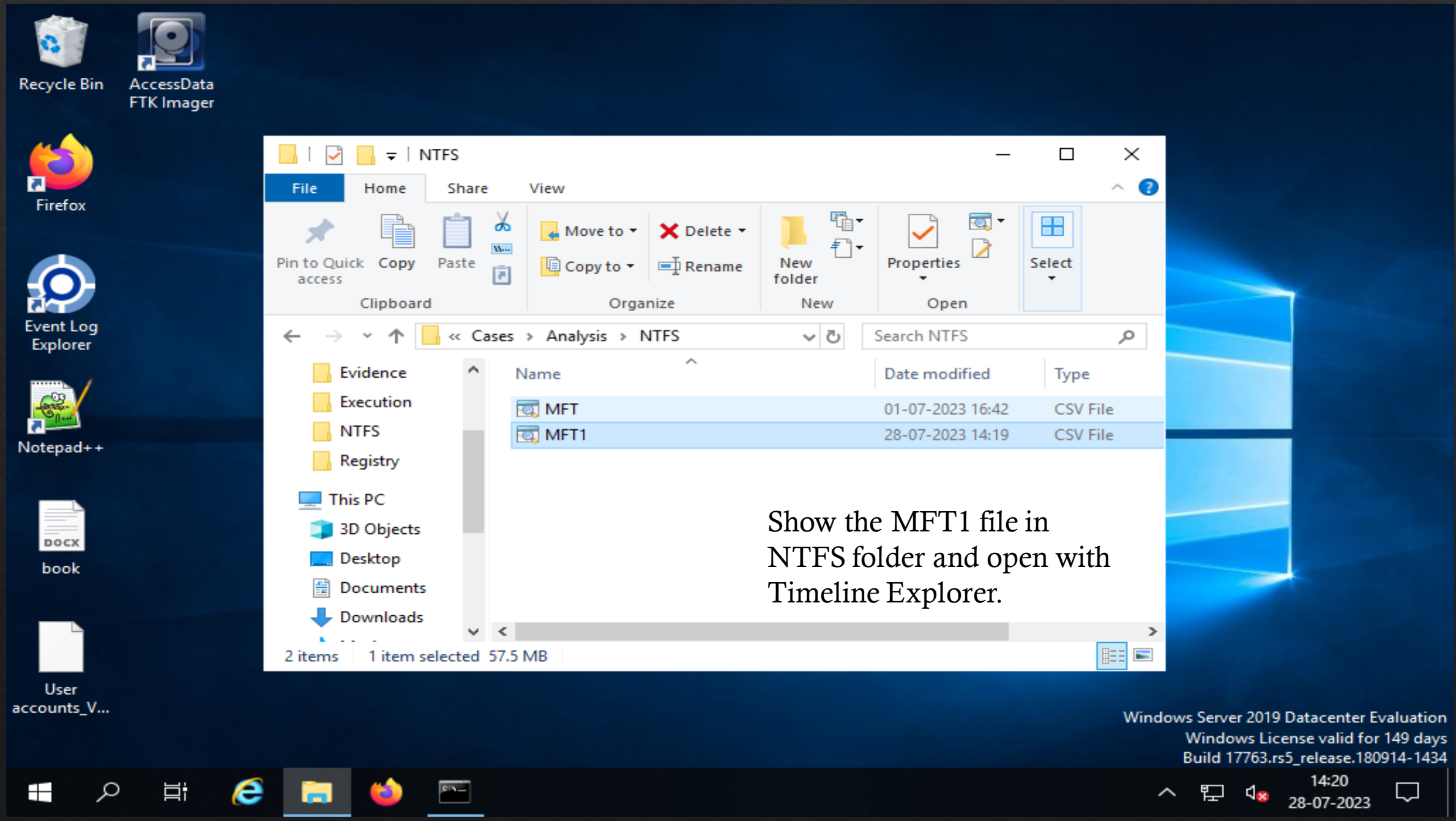
Using this command gathering the information about this file.

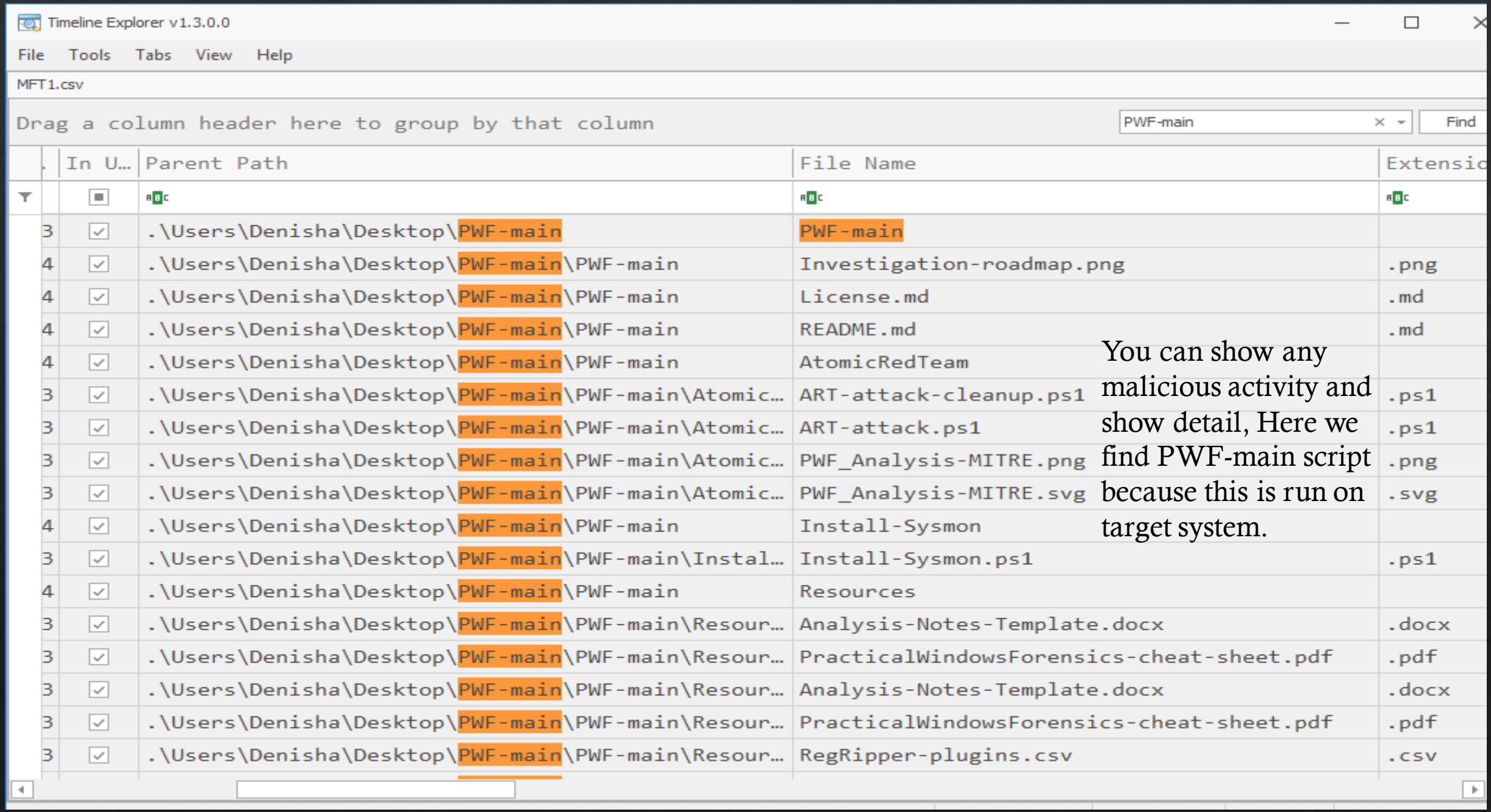

Administrator: C:\Windows\System32\cmd.exe
Last Accessed On: 2023-06-29 05:02:52.1527466
**** FILE NAME ****
Attribute #: 0x3, Size: 0x68, Content size: 0x4A, Name size: 0x0, ContentOffset 0x18. Resident: True
File name: $MFT
Flags: Hidden, System, Name Type: DosWindows, Reparse Value: 0x0, Physical 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



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


Recycle Bin
AccessData FTK Imager
Firefox
Event Log Explorer
Notepad++
book
User accounts_V...
NTFS
File
Home
Share
View
Pin to Quick access
Copy
Paste
Move to
Copy to
Delete
Rename
New folder
Properties
Select
Clipboard
Organize
New
Open
Cases
Analysis
NTFS
Search NTFS
Evidence
Execution
NTFS
Registry
This PC
3D Objects
Desktop
Documents
Downloads
Name
Date modified
Type
MFT
01-07-2023 16:42
CSV File
MFT1
28-07-2023 14:19
CSV File
Show the MFT1 file in NTFS folder and open with Timeline Explorer.
2 items
1 item selected 57.5 MB
Windows Server 2019 Datacenter Evaluation
Windows License valid for 149 days
Build 17763.rs5_release.180914-1434
14:20
28-07-2023



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

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

MFT1.csv

Drag a column header here to group by that column

PWF-main Find

File Size	Created0x10	Created0x30	Last Modified0x10	Last Modified0x30	Last Record Change0x1
=	=	=	=	=	=
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

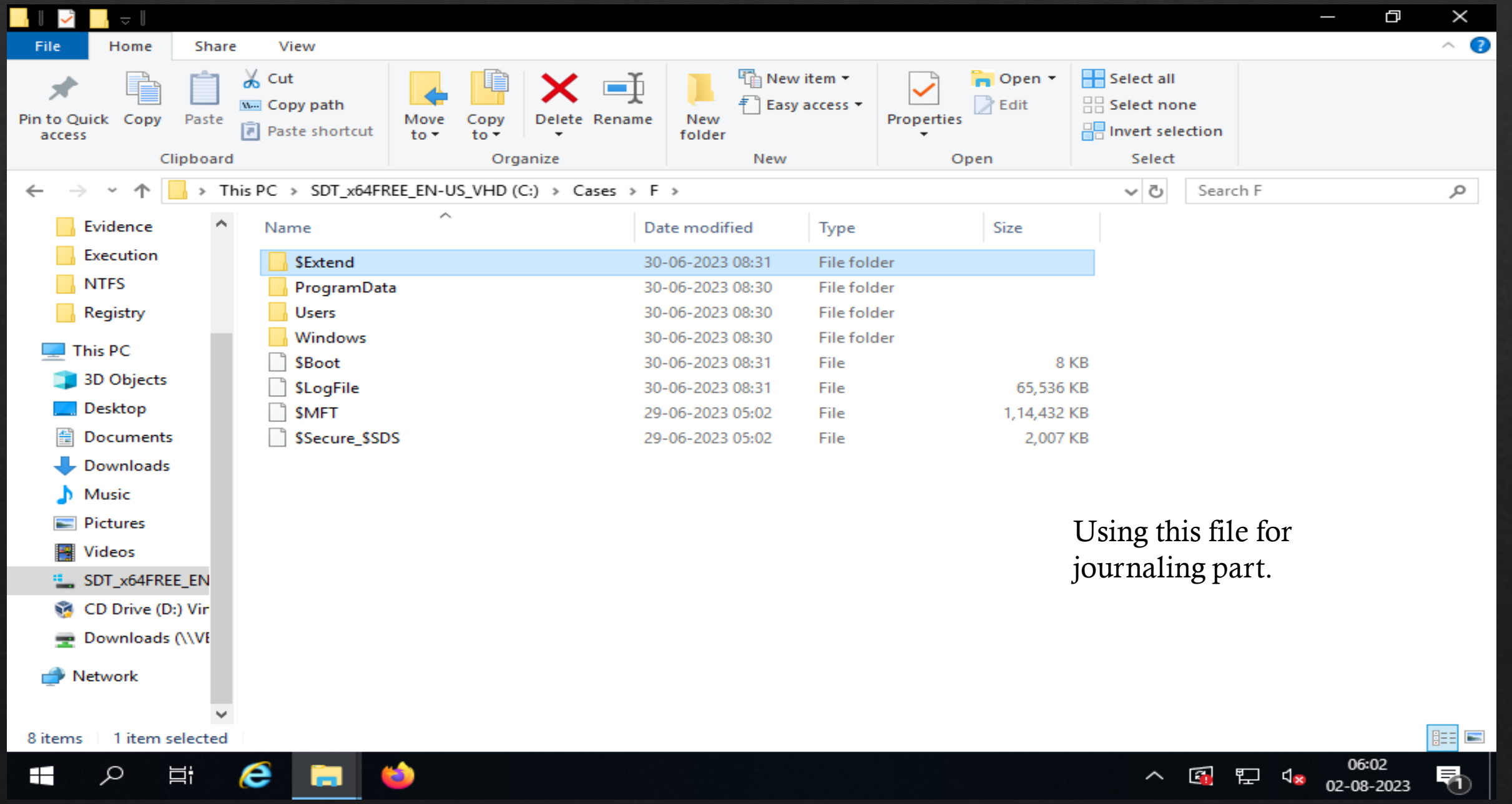
A – Access

C – Changed(last Access $MFT)

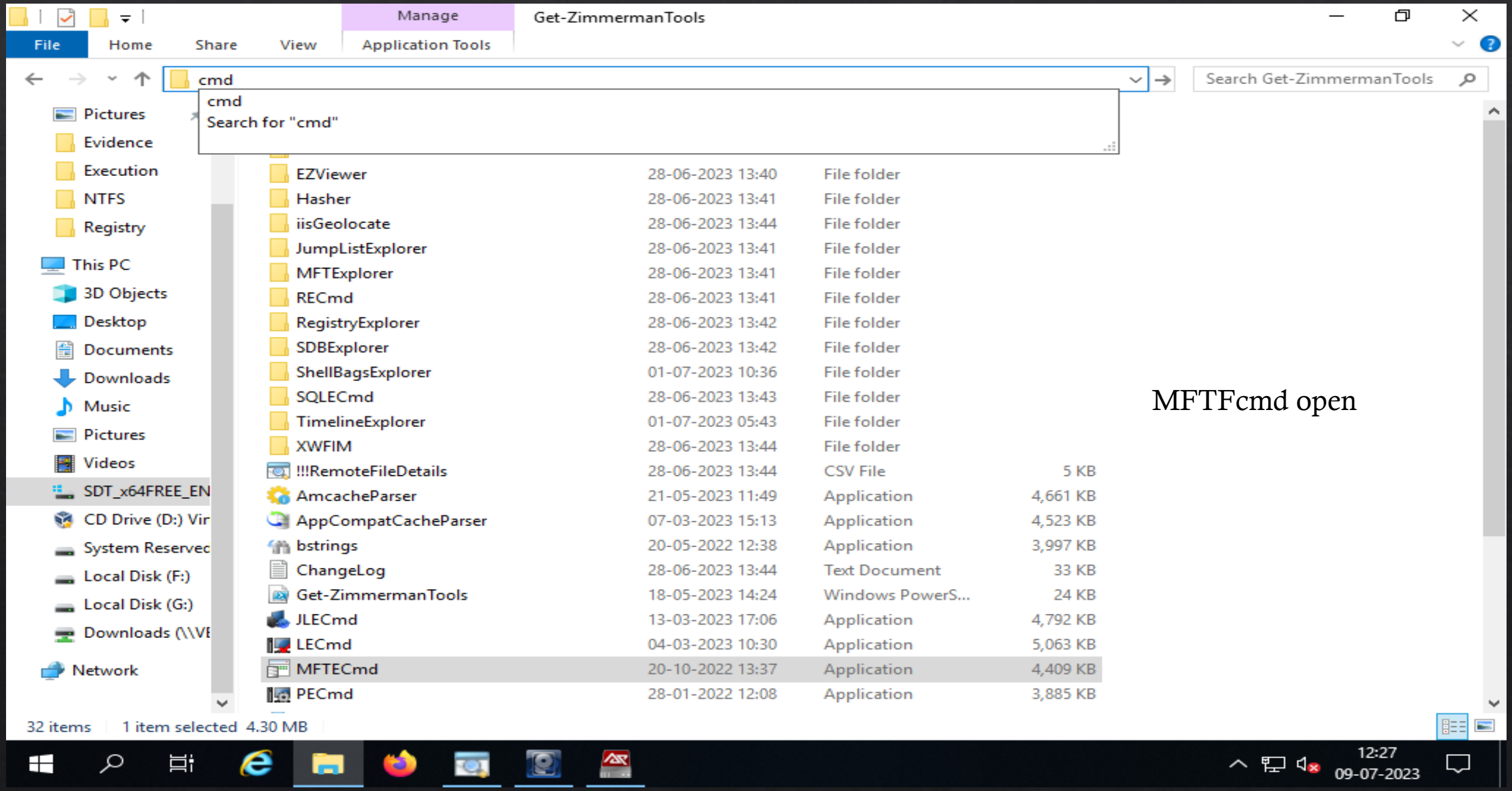
B - (Birth) / Creation

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.

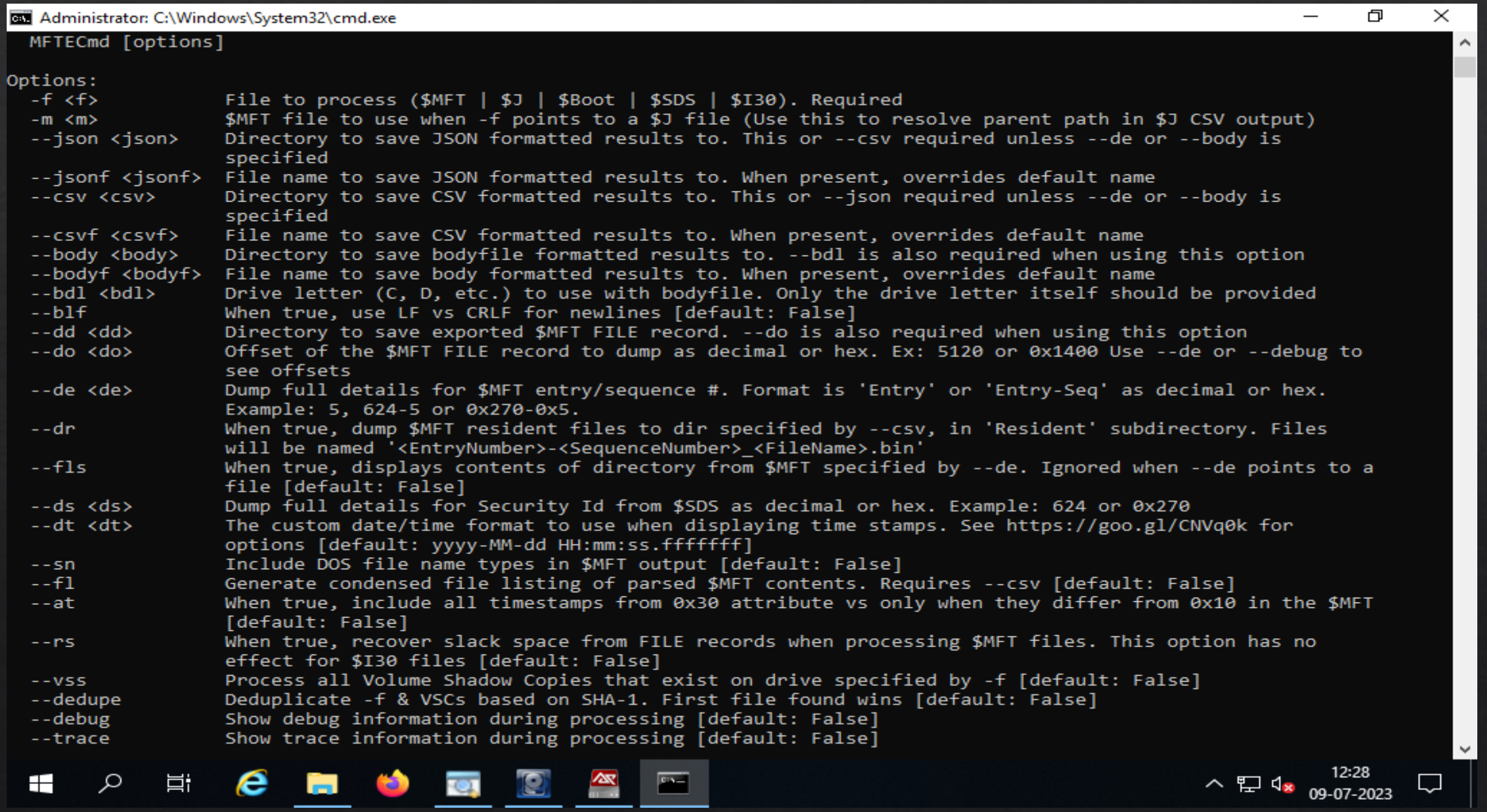
Finding Evidence of deleted filed with USN Journal analysis

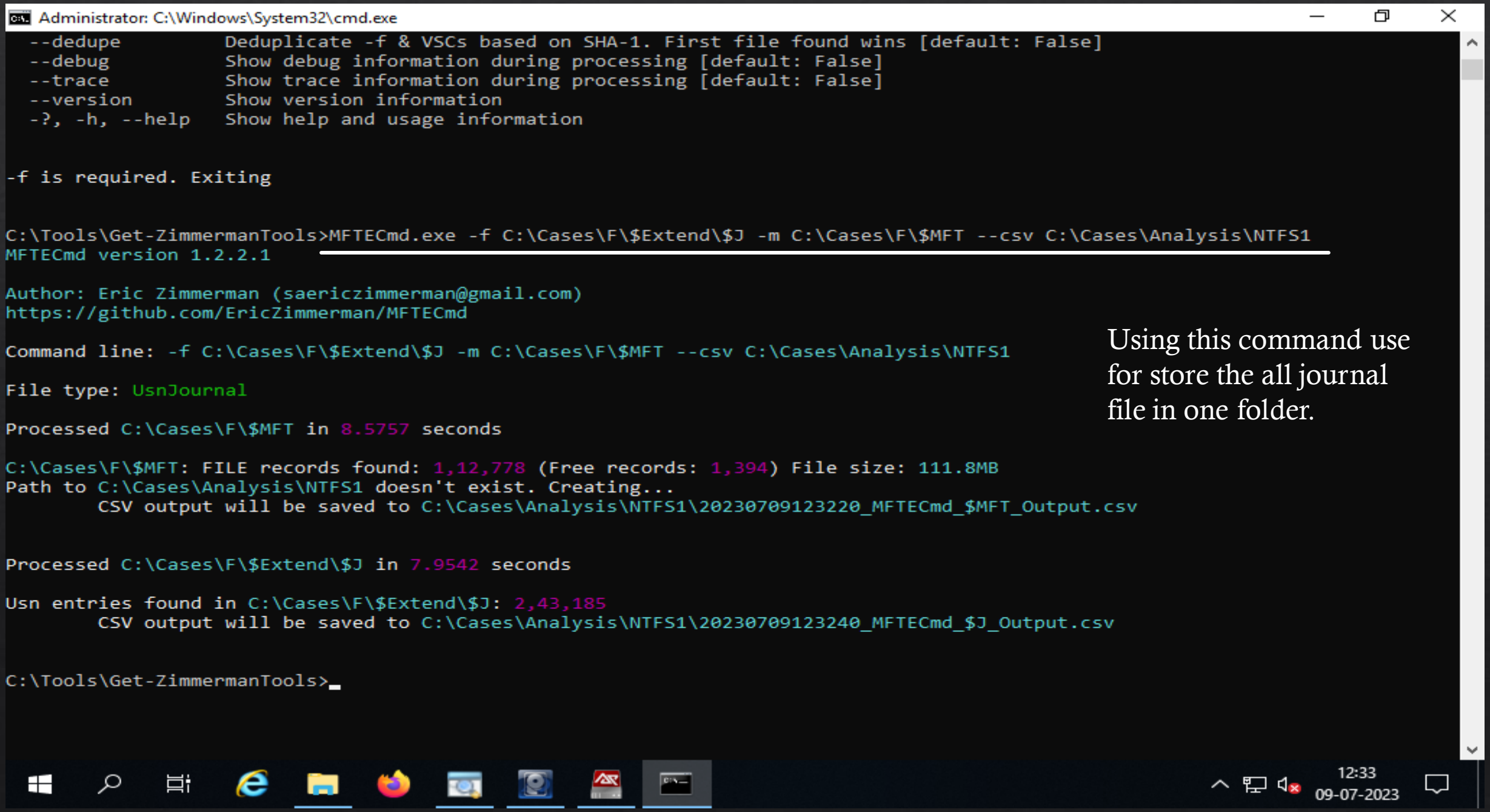


Using this file for journaling part.

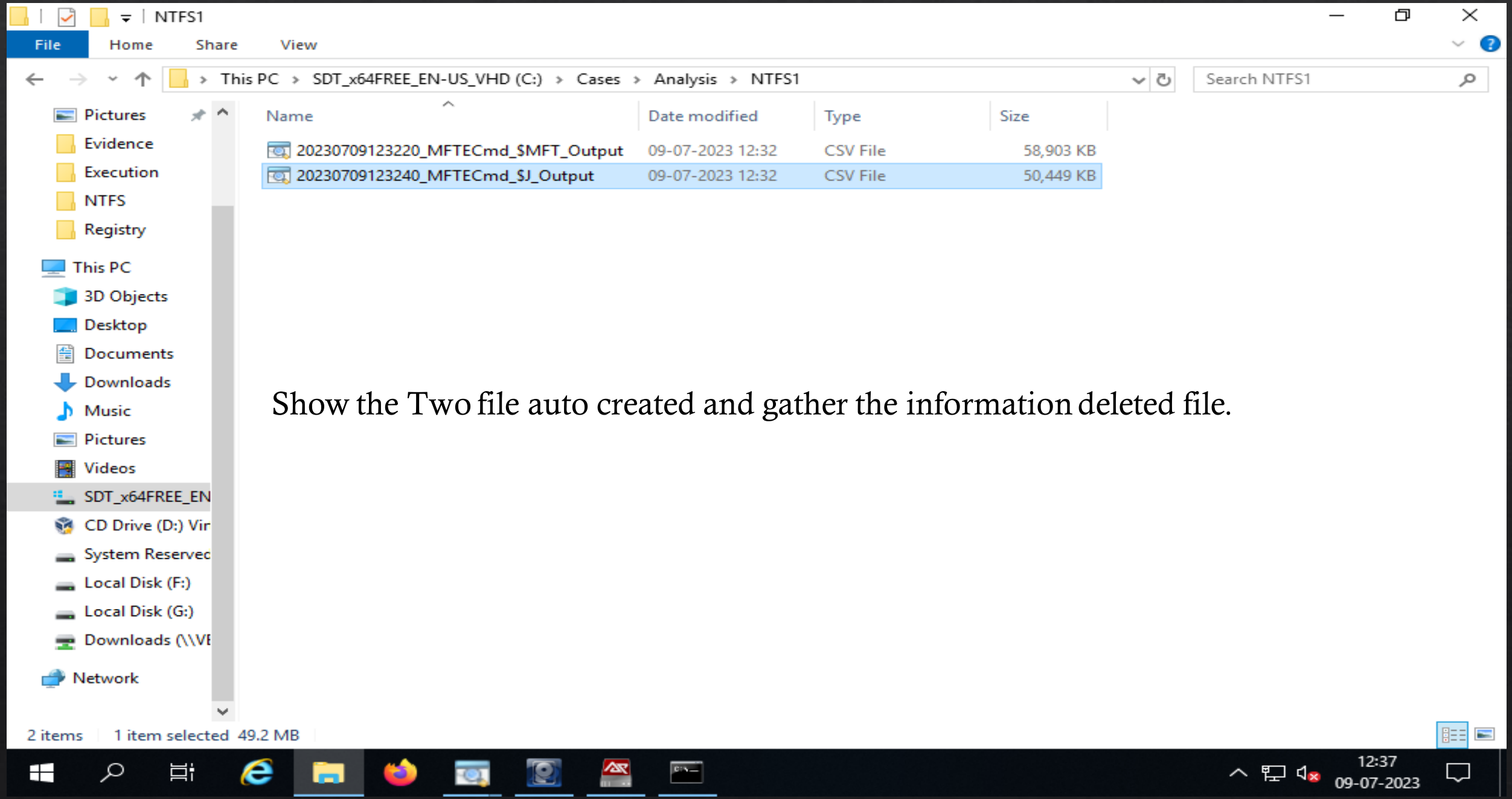


MFTFcmd open


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.fffffff]
--sn Include DOS file name types in $MFT output [default: False]
--fl Generate condensed file listing of parsed $MFT contents. Requires --csv [default: False]
--at When true, include all timestamps from 0x30 attribute vs only when they differ from 0x10 in the $MFT [default: False]
--rs When true, recover slack space from FILE records when processing $MFT files. This option has no effect for $I30 files [default: False]
--vss Process all Volume Shadow Copies that exist on drive specified by -f [default: False]
--dedupe Deduplicate -f & VSCs based on SHA-1. First file found wins [default: False]
--debug Show debug information during processing [default: False]
--trace Show trace information during processing [default: False]
12:28
09-07-2023



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



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

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

20230709123240_MFTECmd_$J_Output.csv

Drag a column header here to group by that column

Enter text to search... Find

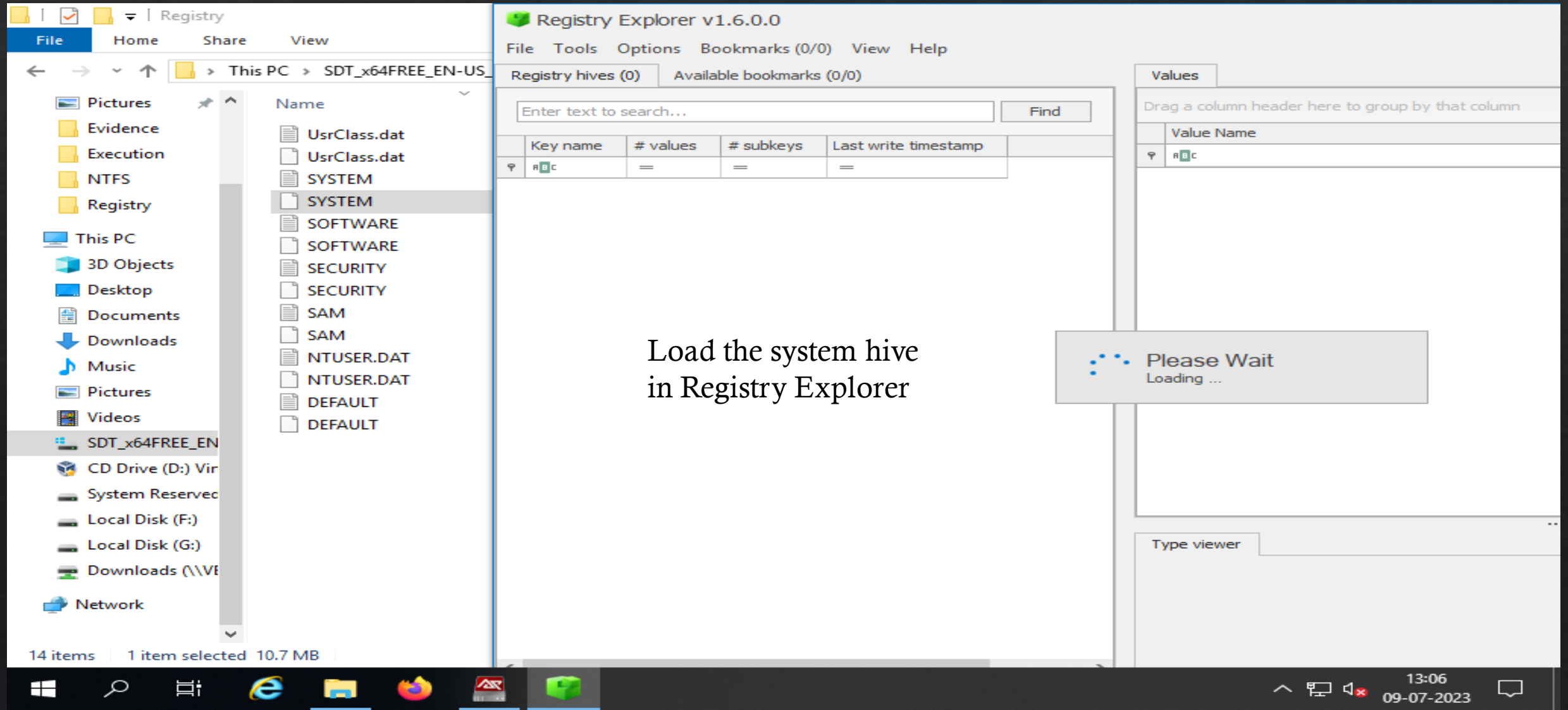
r	Parent Sequence Number	Update Sequence Number	Update Reasons	File A
=	=	=	ABC	ABC
761	1	22959408	HardLinkChange|Close	Arch
761	1	22959536	HardLinkChange|Close	Arch
761	1	22959664	HardLinkChange|Close	Arch
761	1	22959792	HardLinkChange|Close	Arch
761	1	22959920	HardLinkChange|Close	Arch
761	1	22960048	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

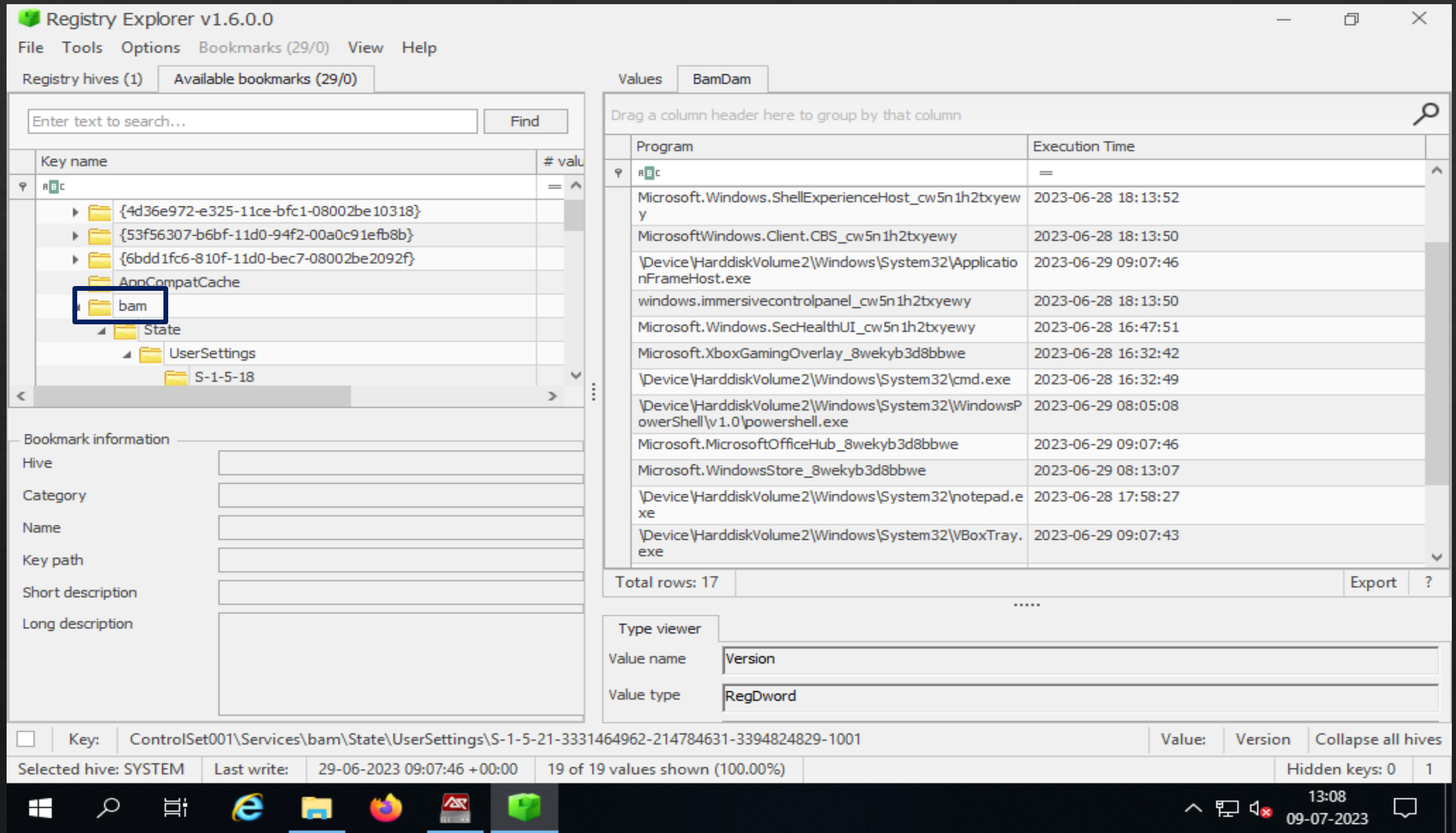
C:\Cases\Analysis\NTFS1\20230709123240_MFTECmd_$J_Output.csv | Total lines 2,43,185 | Visible lines 2,43,185 | Open files: 1 | Search options

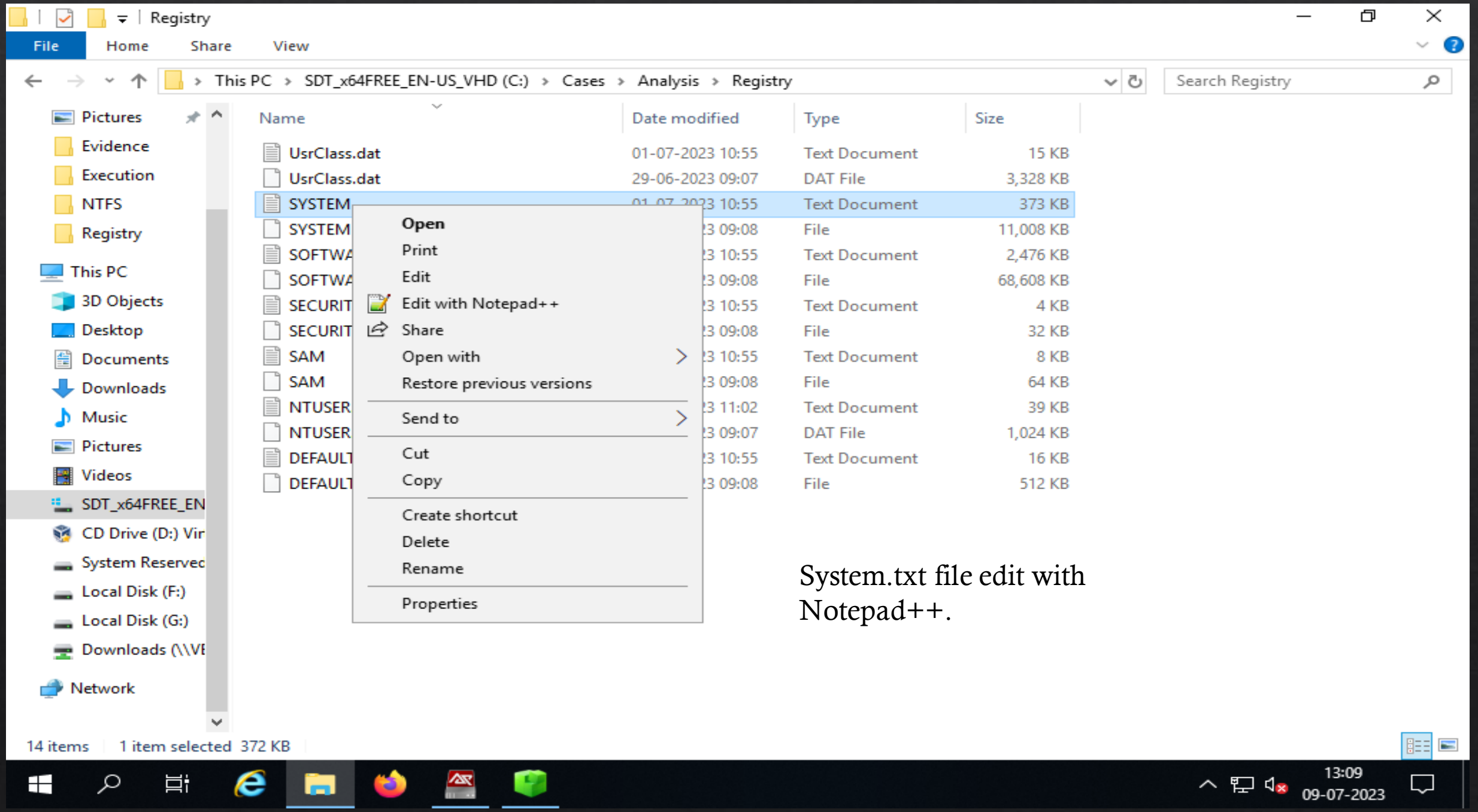
12:40
09-07-2023

Evidence of Execution

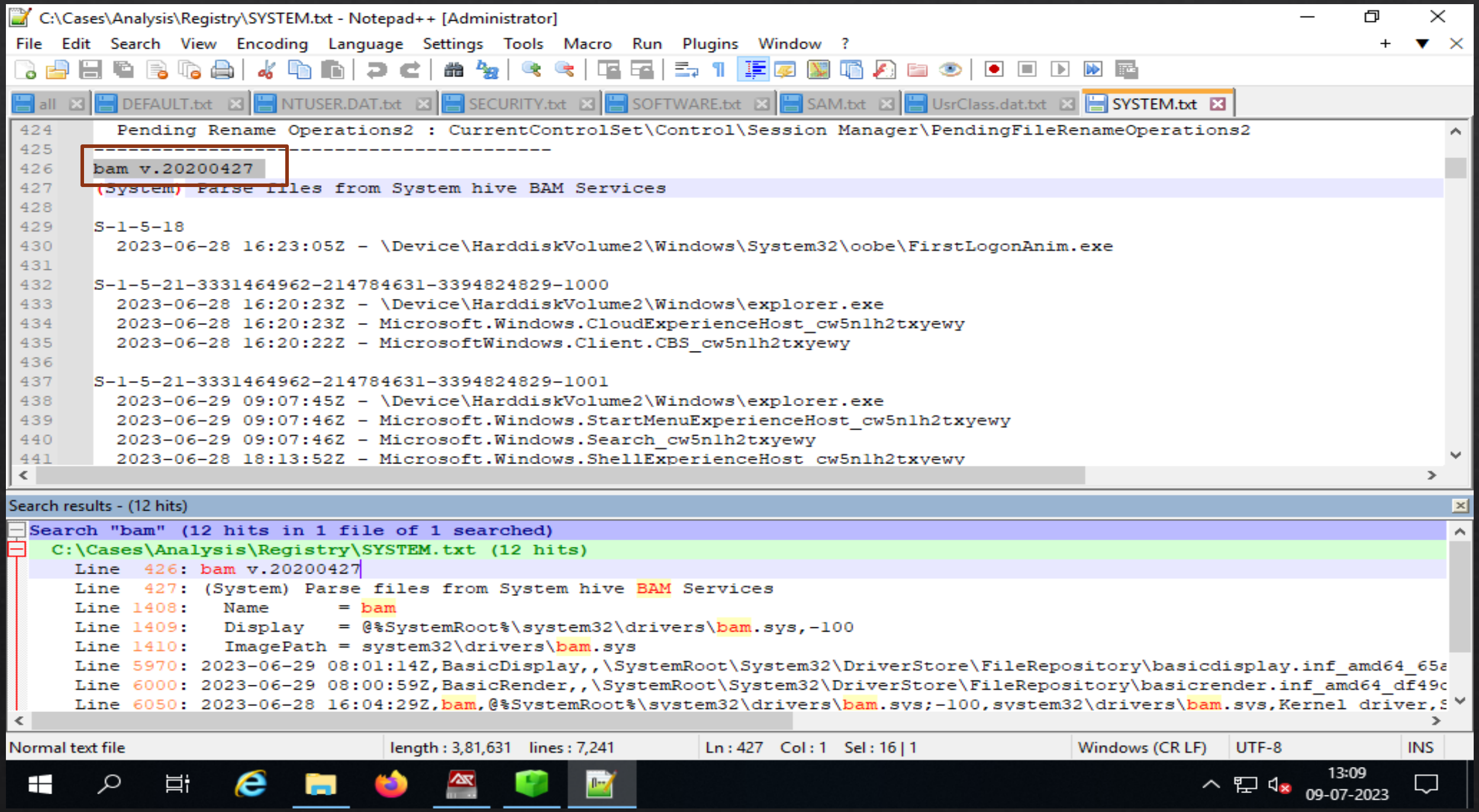
1. BAM (Background Activity Moderator)




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
valu
{4d36e972-e325-11ce-bfc1-08002be10318}
{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
{6bdd1fc6-810f-11d0-bec7-08002be2092f}
AppCompatCache
bam
State
UserSettings
S-1-5-18
Bookmark information
Hive
Category
Name
Key path
Short description
Long description
Values BamDam
Drag a column header here to group by that column
Program
Execution Time
Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy 2023-06-28 18:13:52
MicrosoftWindows.Client.CBS_cw5n1h2txyewy 2023-06-28 18:13:50
\Device\HarddiskVolume2\Windows\System32\ApplicationFrameHost.exe 2023-06-29 09:07:46
windows.immersivecontrolpanel_cw5n1h2txyewy 2023-06-28 18:13:50
Microsoft.Windows.SecHealthUI_cw5n1h2txyewy 2023-06-28 16:47:51
Microsoft.XboxGamingOverlay_8wekyb3d8bbwe 2023-06-28 16:32:42
\Device\HarddiskVolume2\Windows\System32\cmd.exe 2023-06-28 16:32:49
\Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe 2023-06-29 08:05:08
Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe 2023-06-29 09:07:46
Microsoft.WindowsStore_8wekyb3d8bbwe 2023-06-29 08:13:07
\Device\HarddiskVolume2\Windows\System32\notepad.exe 2023-06-28 17:58:27
\Device\HarddiskVolume2\Windows\System32\VBoxTray.exe 2023-06-29 09:07:43
Total rows: 17
Export
?
Type viewer
Value name
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

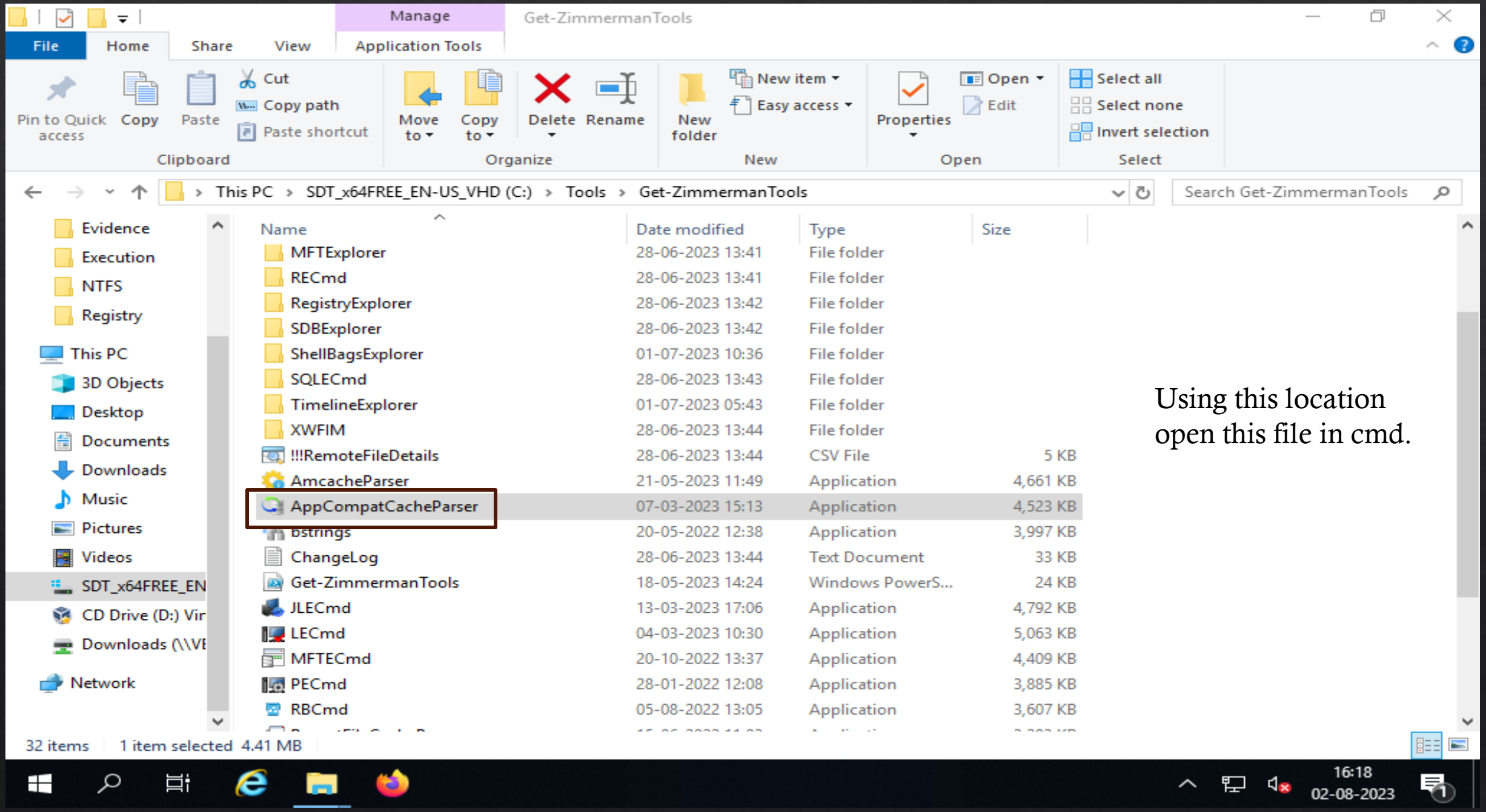


System.txt file edit with Notepad++.


C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
all DEFAULT.txt NTUSER.DAT.txt SECURITY.txt SOFTWARE.txt SAM.txt UsrClass.dat.txt SYSTEM.txt
424 Pending Rename Operations2 : CurrentControlSet\Control\Session Manager\PendingFileRenameOperations2
425 ----------
426 bam v.20200427
427 (System) Parse files from System hive BAM Services
428
429 S-1-5-18
430 2023-06-28 16:23:05Z - \Device\HarddiskVolume2\Windows\System32\oobe\FirstLogonAnim.exe
431
432 S-1-5-21-3331464962-214784631-3394824829-1000
433 2023-06-28 16:20:23Z - \Device\HarddiskVolume2\Windows\explorer.exe
434 2023-06-28 16:20:23Z - Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy
435 2023-06-28 16:20:22Z - MicrosoftWindows.Client.CBS_cw5n1h2txyewy
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_cw5n1h2txyewy
440 2023-06-29 09:07:46Z - Microsoft.Windows.Search_cw5n1h2txyewy
441 2023-06-28 18:13:52Z - Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy
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.sys,Kernel driver,s
Normal text file length : 3,81,631 lines : 7,241 Ln : 427 Col : 1 Sel : 16 | 1 Windows (CR LF) UTF-8 INS
13:09
09-07-2023

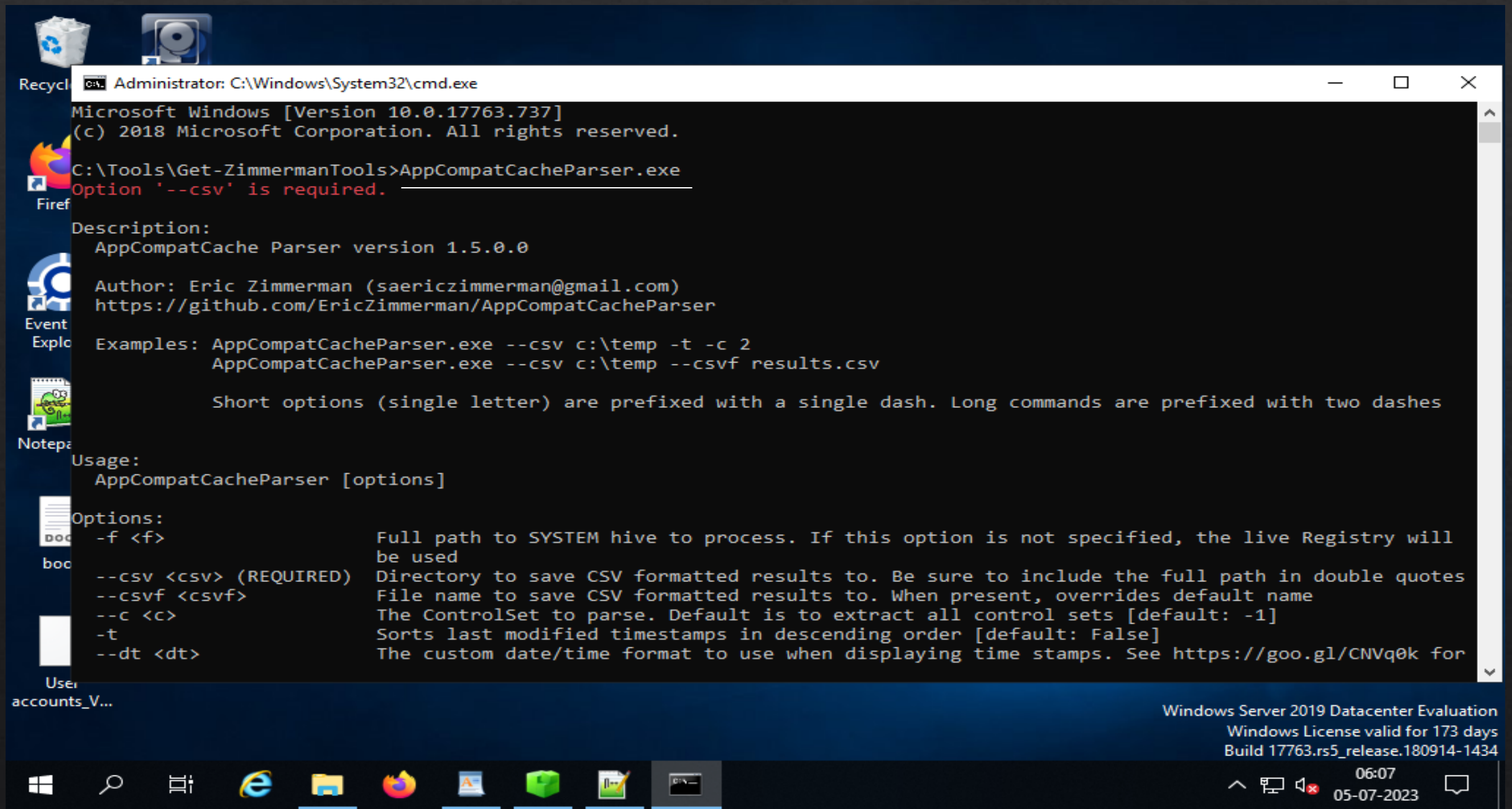
2. AppCompactcache Analysis/Shimcache

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

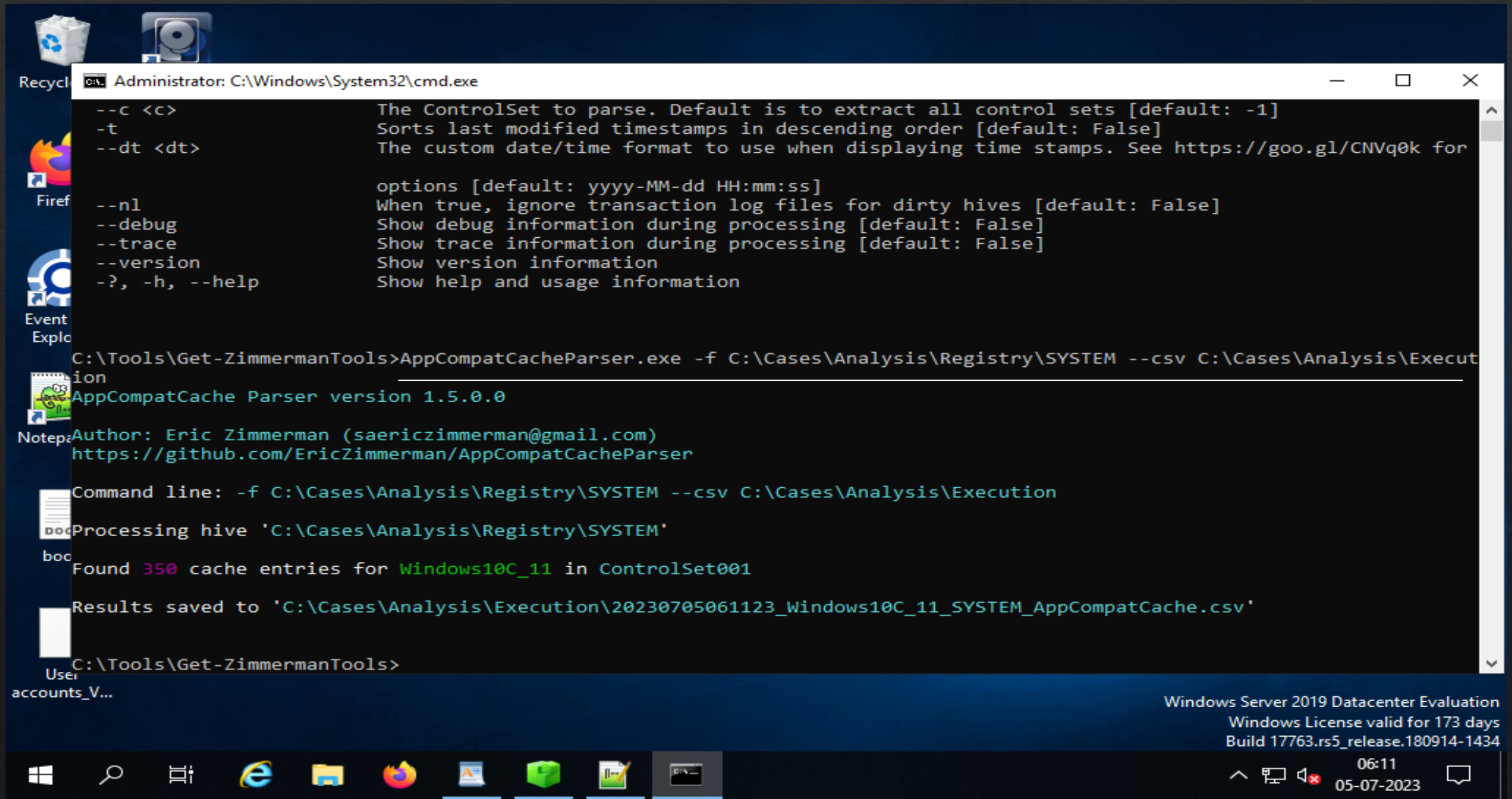


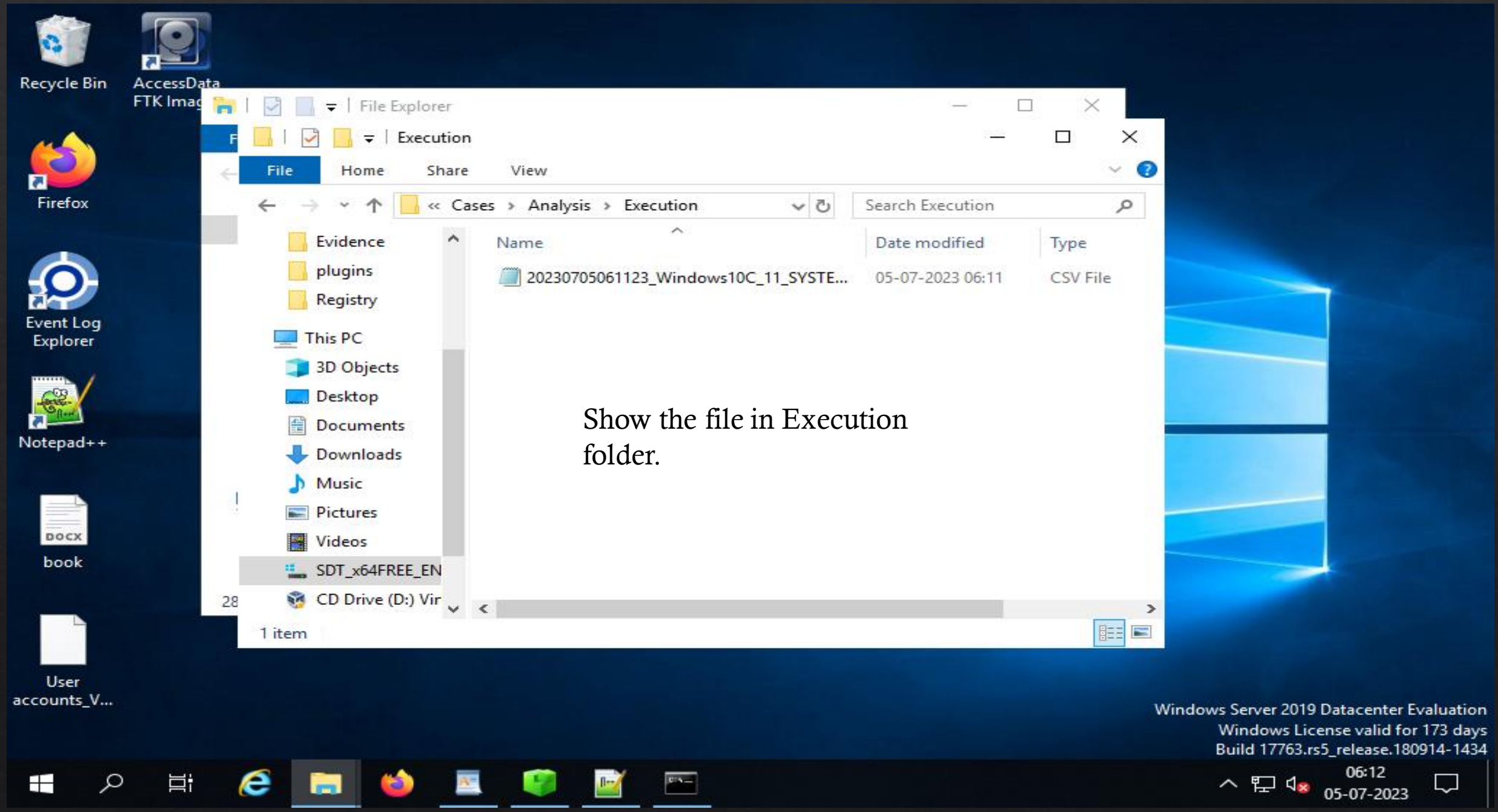
Using this location open this file in cmd.

Go to the Appcompatcacheparser.exe in cmd

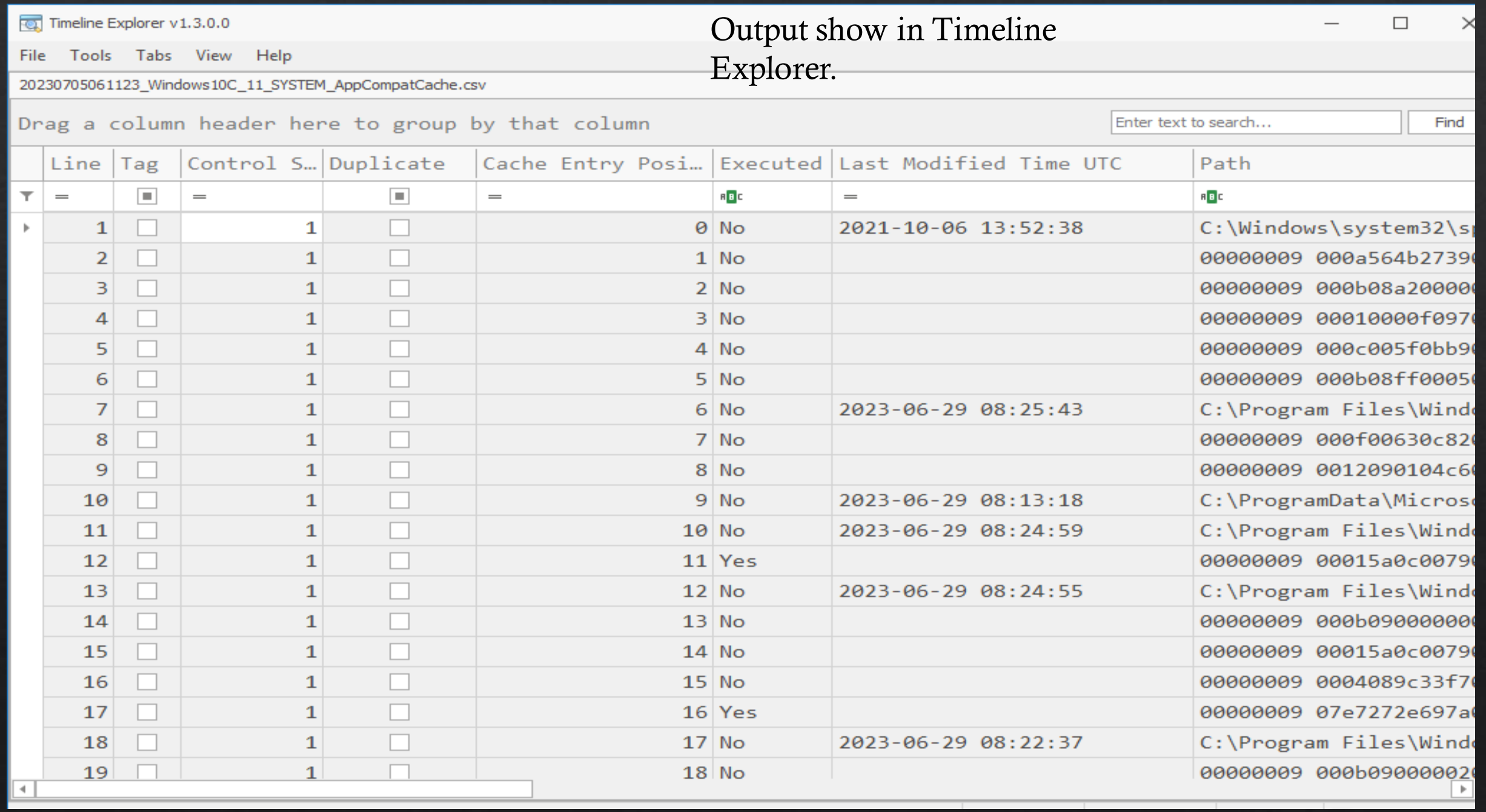


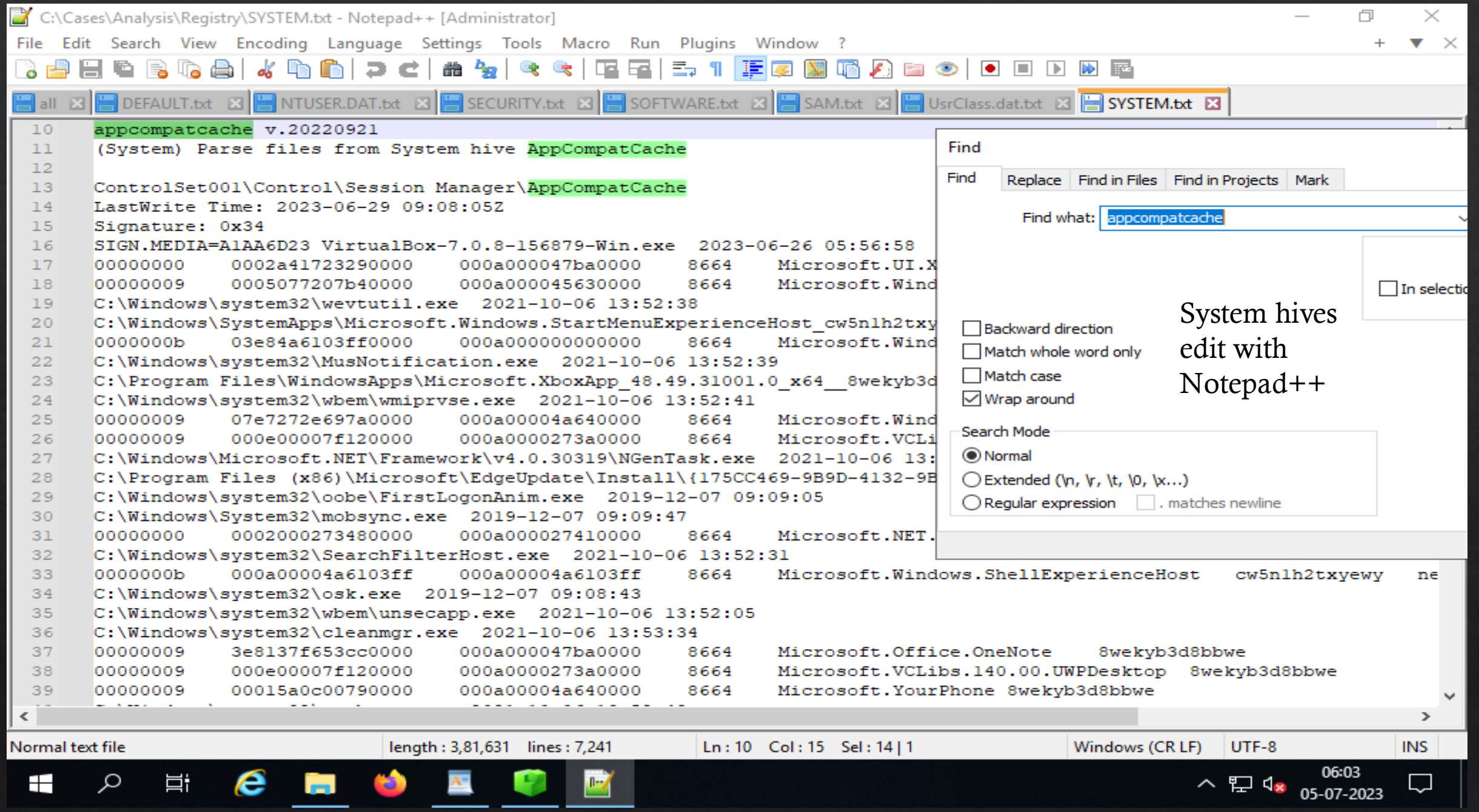
Create the folder Execution in Analysis and run this command and store the output in Execution folder.




Recycle Bin
AccessData FTK Imag
Firefox
Event Log Explorer
Notepad++
book
User accounts_V...
File Explorer
Execution
File
Home
Share
View
Cases › Analysis › Execution
Search Execution
Evidence
plugins
Registry
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
SDT_x64FREE_EN
CD Drive (D:) Vir
Name
Date modified
Type
20230705061123_Windows10C_11_SYSTE...
05-07-2023 06:11
CSV File
1 item
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

Output show in Timeline Explorer.

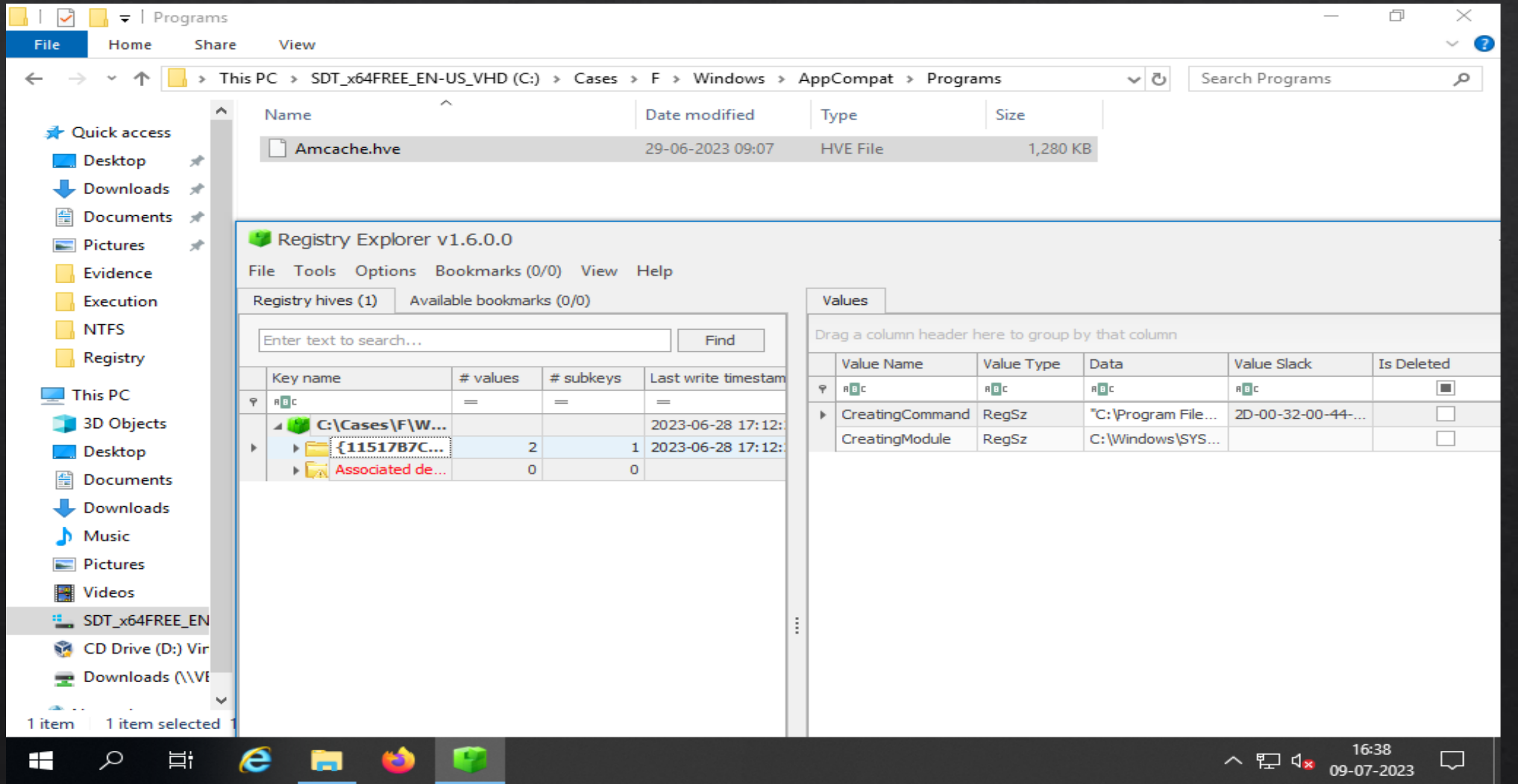


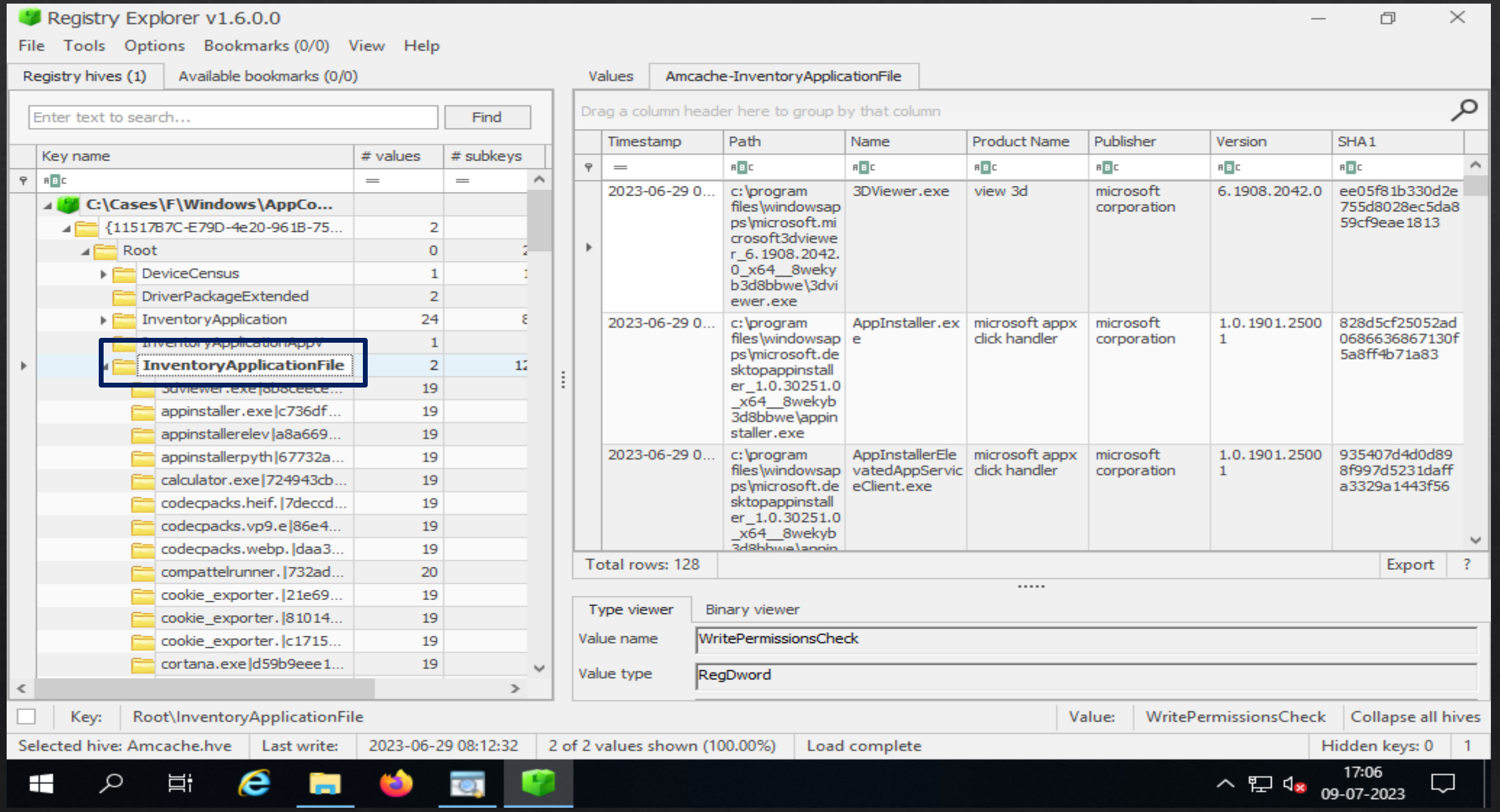

C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
all DEFAULT.txt NTUSER.DAT.txt SECURITY.txt SOFTWARE.txt SAM.txt UsrClass.dat.txt SYSTEM.txt
10 appcompatcache v.20220921
11 (System) Parse files from System hive AppCompatCache
12
13 ControlSet001\Control\Session Manager\AppCompatCache
14 LastWrite Time: 2023-06-29 09:08:05Z
15 Signature: 0x34
16 SIGN.MEDIA=A1AA6D23 VirtualBox-7.0.8-156879-Win.exe 2023-06-26 05:56:58
17 00000000 0002a41723290000 000a000047ba0000 8664 Microsoft.UI.X
18 00000009 0005077207b40000 000a000045630000 8664 Microsoft.Wind
19 C:\Windows\system32\wevtutil.exe 2021-10-06 13:52:38
20 C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_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 Replace Find in Files Find in Projects Mark
Find what: appcompatcache
In selectio
Backward direction
Match whole word only
Match case
Wrap around
Search Mode
Normal
Extended (\n, \r, \t, \0, \x...)
Regular expression . matches newline
System hives edit with Notepad++
Normal text file length : 3,81,631 lines : 7,241 Ln : 10 Col : 15 Sel : 14 | 1 Windows (CR LF) UTF-8 INS
06:03 05-07-2023

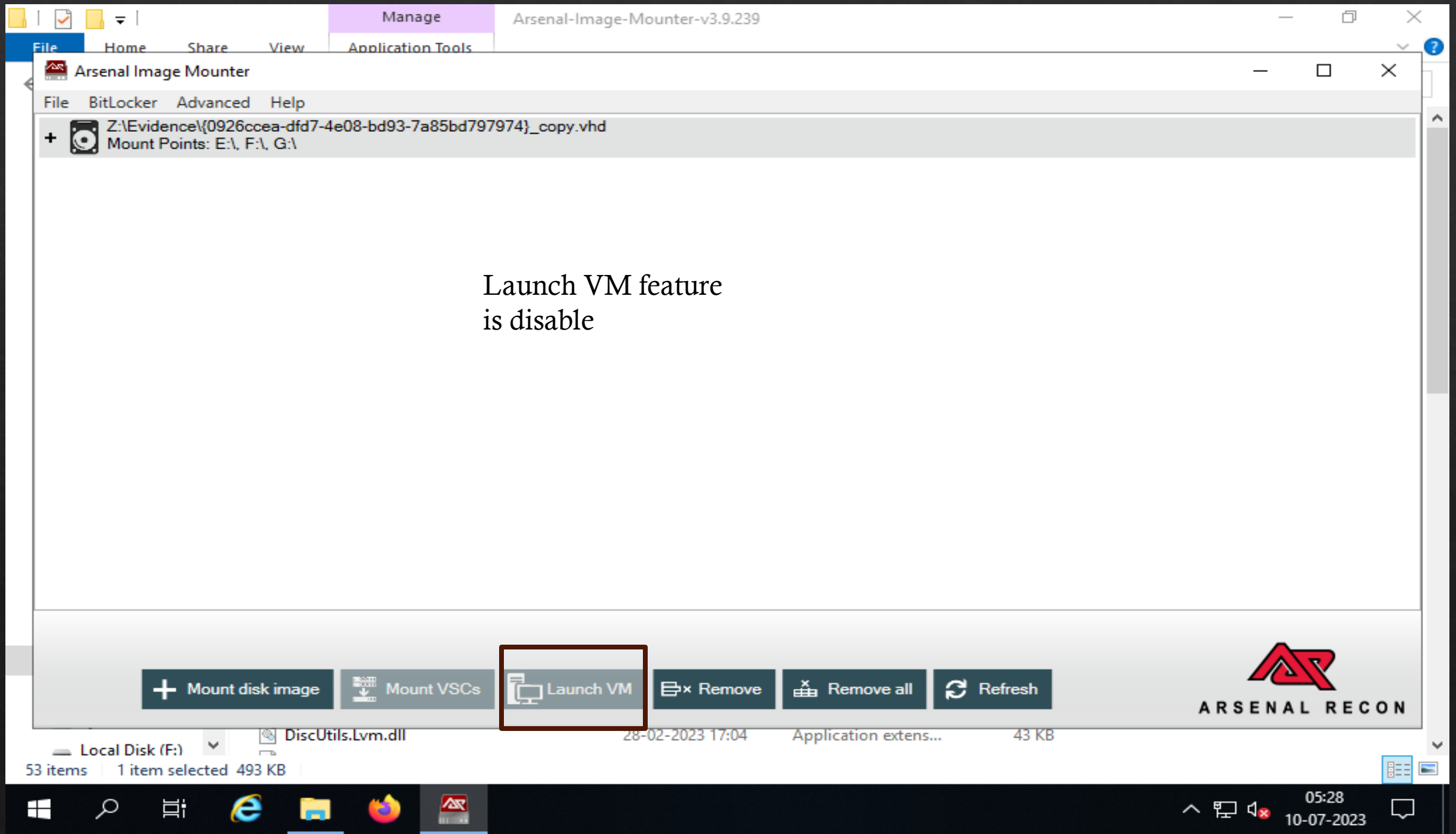
3.Analyzing the Amcache with AmcacheParser

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

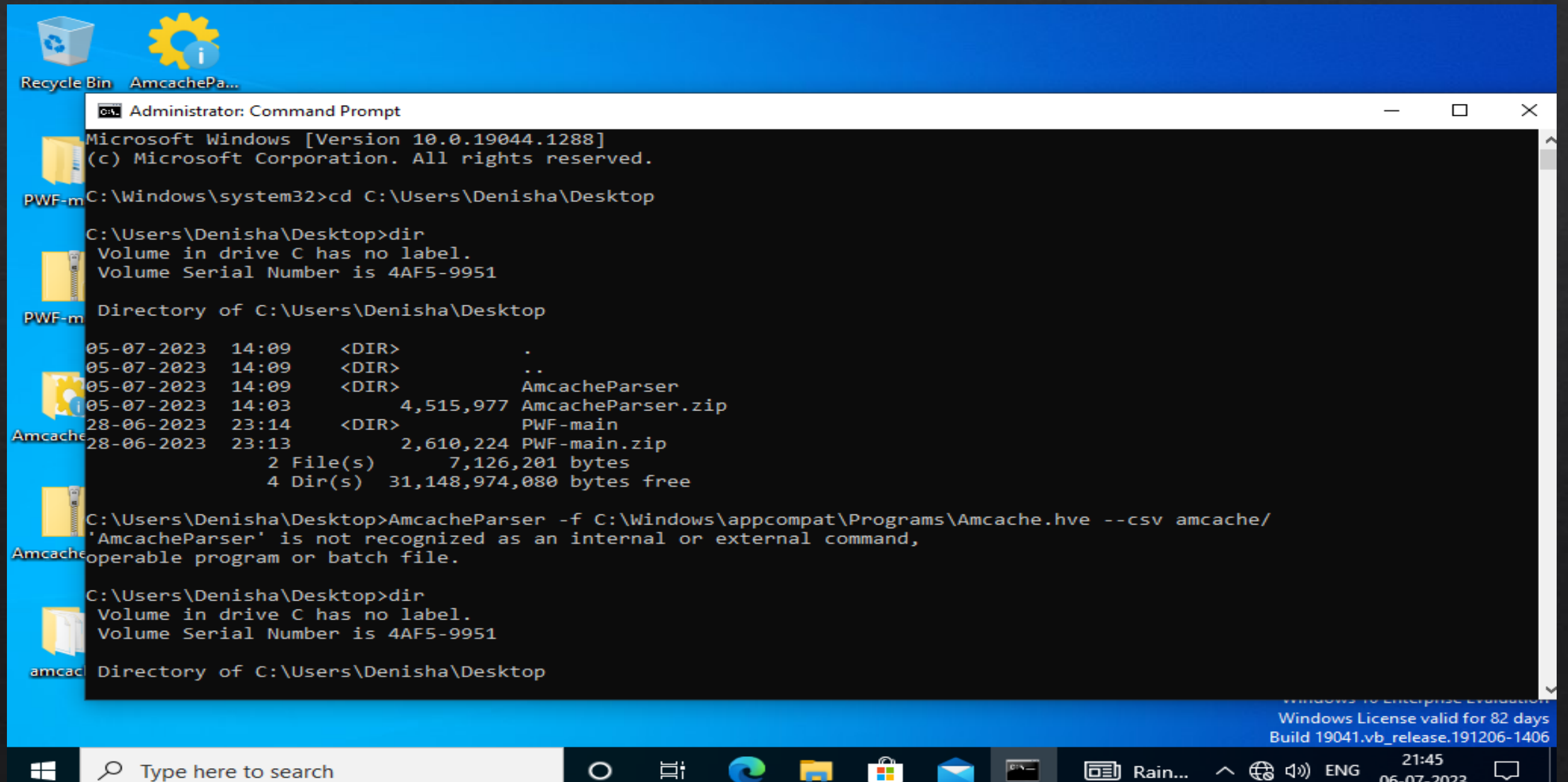
Load the Amcache.hve on Registry Explorer

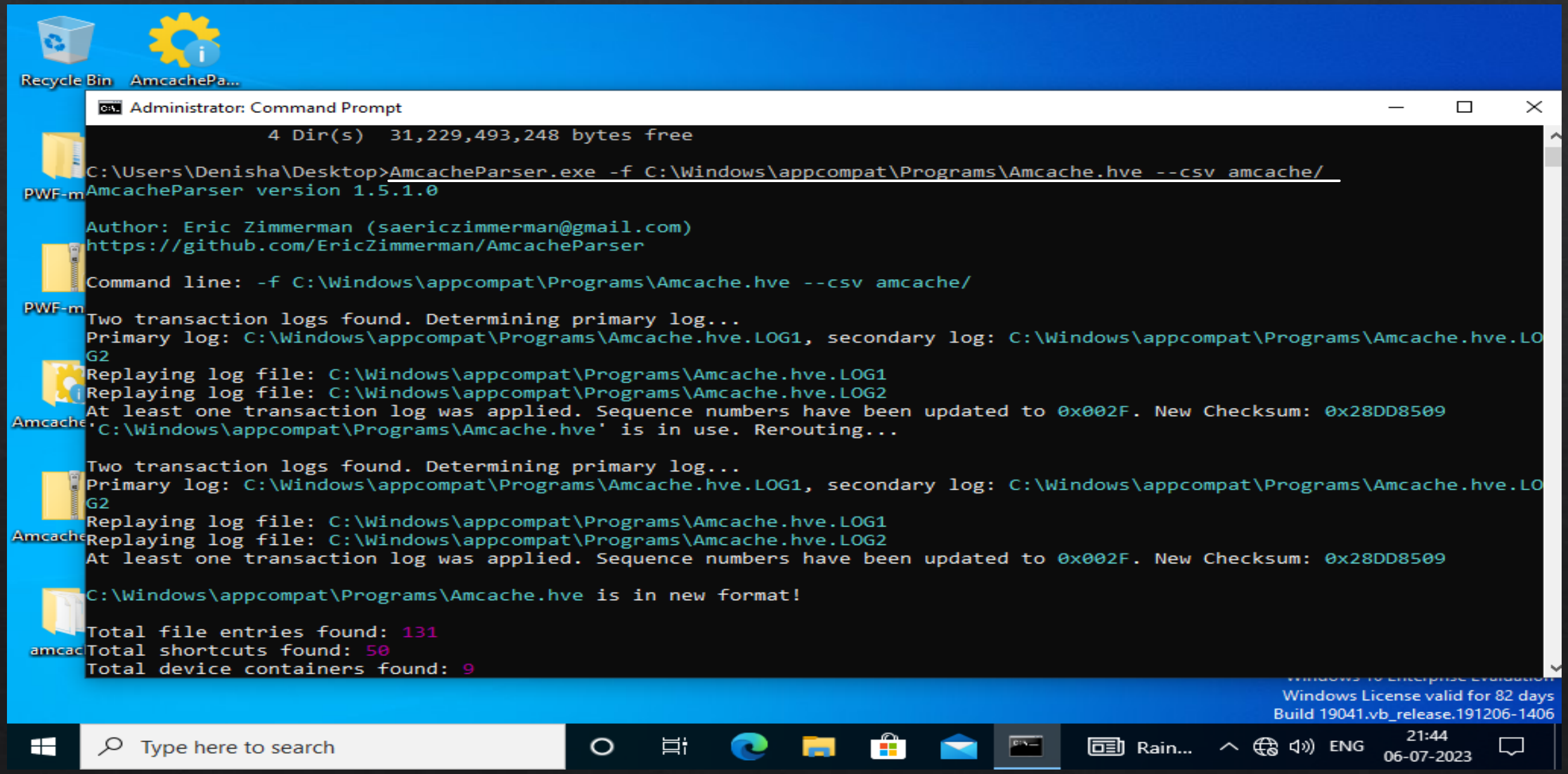



Registry Explorer v1.6.0.0
File Tools Options Bookmarks (0/0) View Help
Registry hives (1) Available bookmarks (0/0)
Enter text to search... Find
Key name # values # subkeys
C:\Cases\F\Windows\AppCo...
{11517B7C-E79D-4e20-961B-75... 2
Root 0
DeviceCensus 1
DriverPackageExtended 2
InventoryApplication 24
InventoryApplicationFile 2
appinstaller.exe|c736df... 19
appinstallerelev|a8a669... 19
appinstallerpyth|67732a... 19
calculator.exe|724943cb... 19
codecpacks.heif.|7deccd... 19
codecpacks.vp9.e|86e4... 19
codecpacks.webp.|daa3... 19
compattelrunner.|732ad... 20
cookie_exporter.|21e69... 19
cookie_exporter.|81014... 19
cookie_exporter.|c1715... 19
cortana.exe|d59b9eee1... 19
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.desktopappinstaller_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.desktopappinstaller_1.0.30251.0_x64__8wekyb3d8bbwe\appinstaller.exe 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

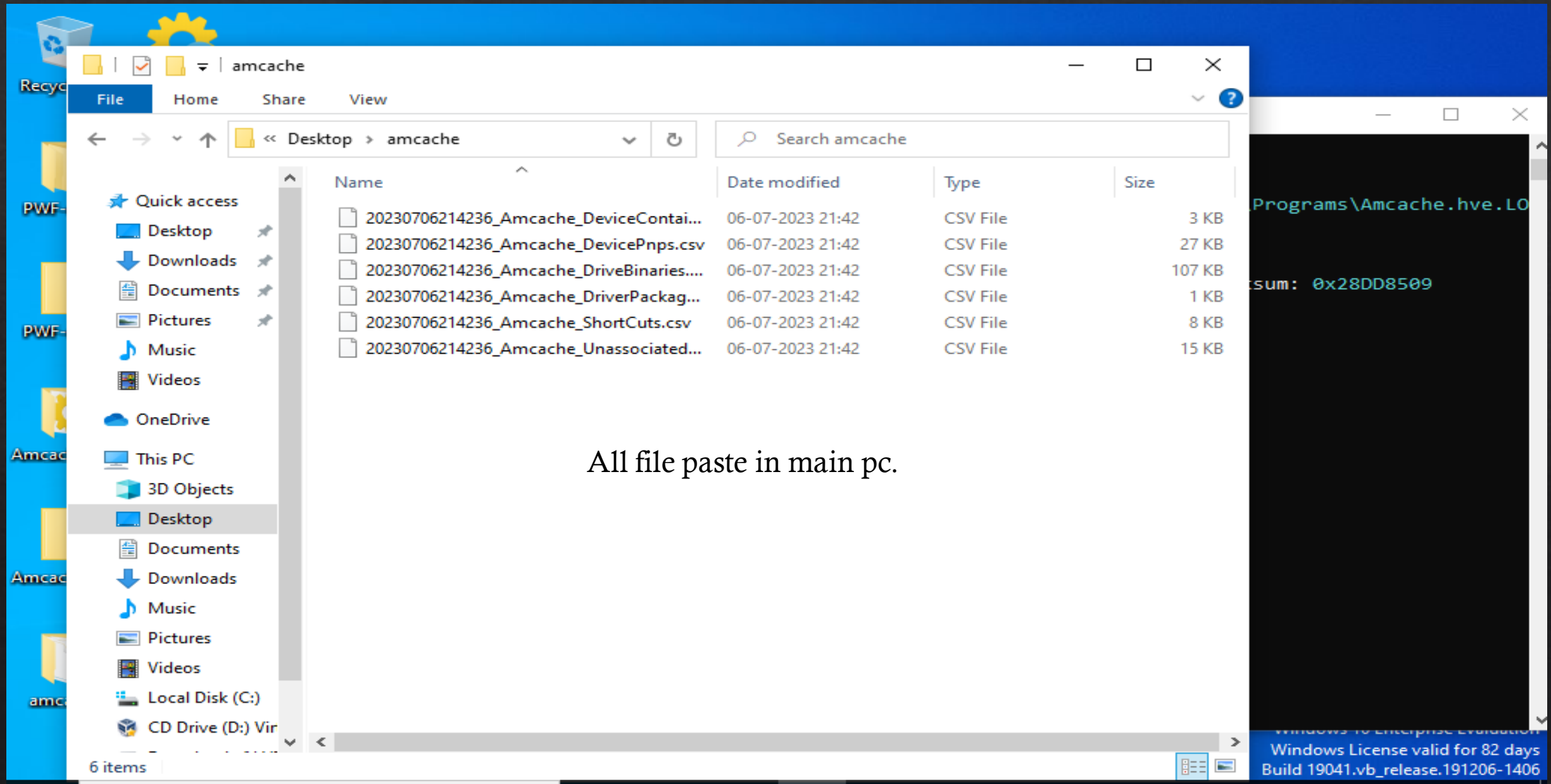

Manage
Arsenal-Image-Mounter-v3.9.239
File
Home
Share
View
Application Tools
Arsenal Image Mounter
File
BitLocker
Advanced
Help
Z:\Evidence\{0926ccea-dfd7-4e08-bd93-7a85bd797974}_copy.vhd
Mount Points: E:\, F:\, G:\
Launch VM feature
is disable
Mount disk image
Mount VSCs
Launch VM
Remove
Remove all
Refresh
ARSENAL RECON
DiscUtils.Lvm.dll
28-02-2023 17:04
Application extens...
43 KB
Local Disk (F:)
53 items
1 item selected 493 KB
05:28
10-07-2023

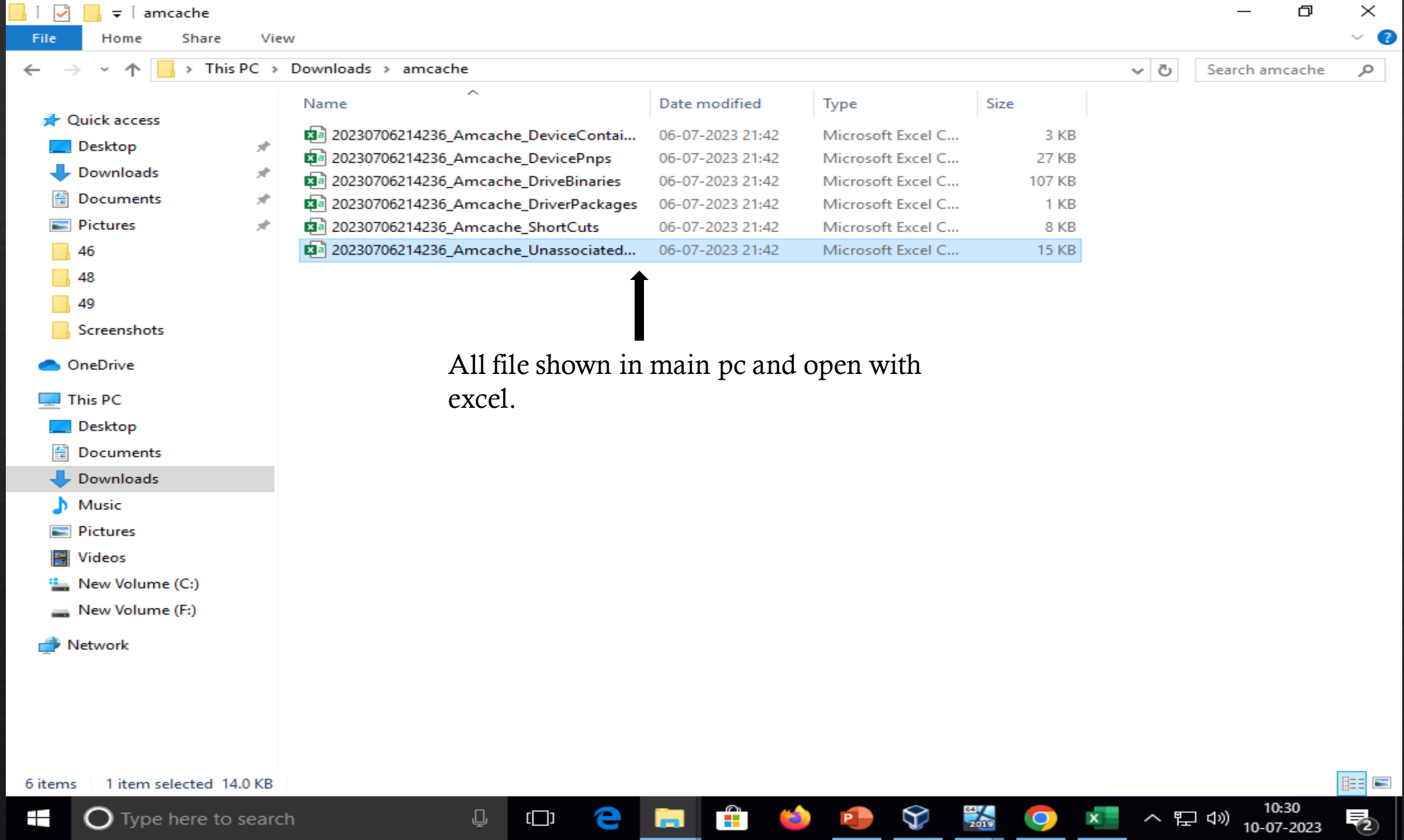
Go to the target system and Download the Amcache in link https://ericzimmerman.github.io/#!index.md and open cmd with Run as a Administrator.

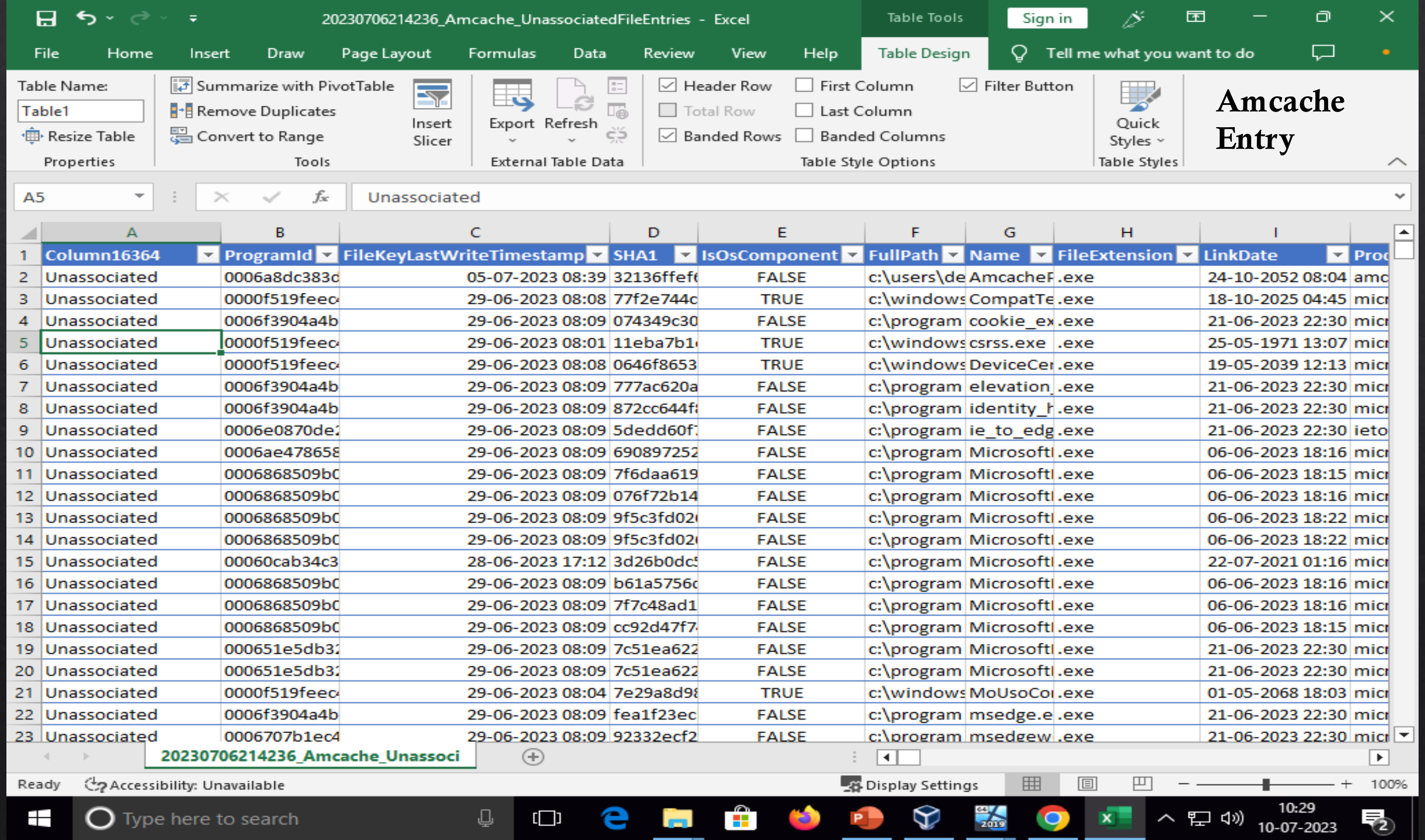



Recycle Bin
AmcachePa...
Administrator: Command Prompt
4 Dir(s) 31,229,493,248 bytes free
C:\Users\Denisha\Desktop>AmcacheParser.exe -f C:\Windows\appcompat\Programs\Amcache.hve --csv amcache/
AmcacheParser version 1.5.1.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AmcacheParser
Command line: -f C:\Windows\appcompat\Programs\Amcache.hve --csv amcache/
Two transaction logs found. Determining primary log...
Primary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG1, secondary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
At least one transaction log was applied. Sequence numbers have been updated to 0x002F. New Checksum: 0x28DD8509
'C:\Windows\appcompat\Programs\Amcache.hve' is in use. Rerouting...
Two transaction logs found. Determining primary log...
Primary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG1, secondary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
At least one transaction log was applied. Sequence numbers have been updated to 0x002F. New Checksum: 0x28DD8509
C:\Windows\appcompat\Programs\Amcache.hve is in new format!
Total file entries found: 131
Total shortcuts found: 50
Total device containers found: 9
Windows License valid for 82 days
Build 19041.vb_release.191206-1406
Type here to search
Rain...
ENG
21:44
06-07-2023

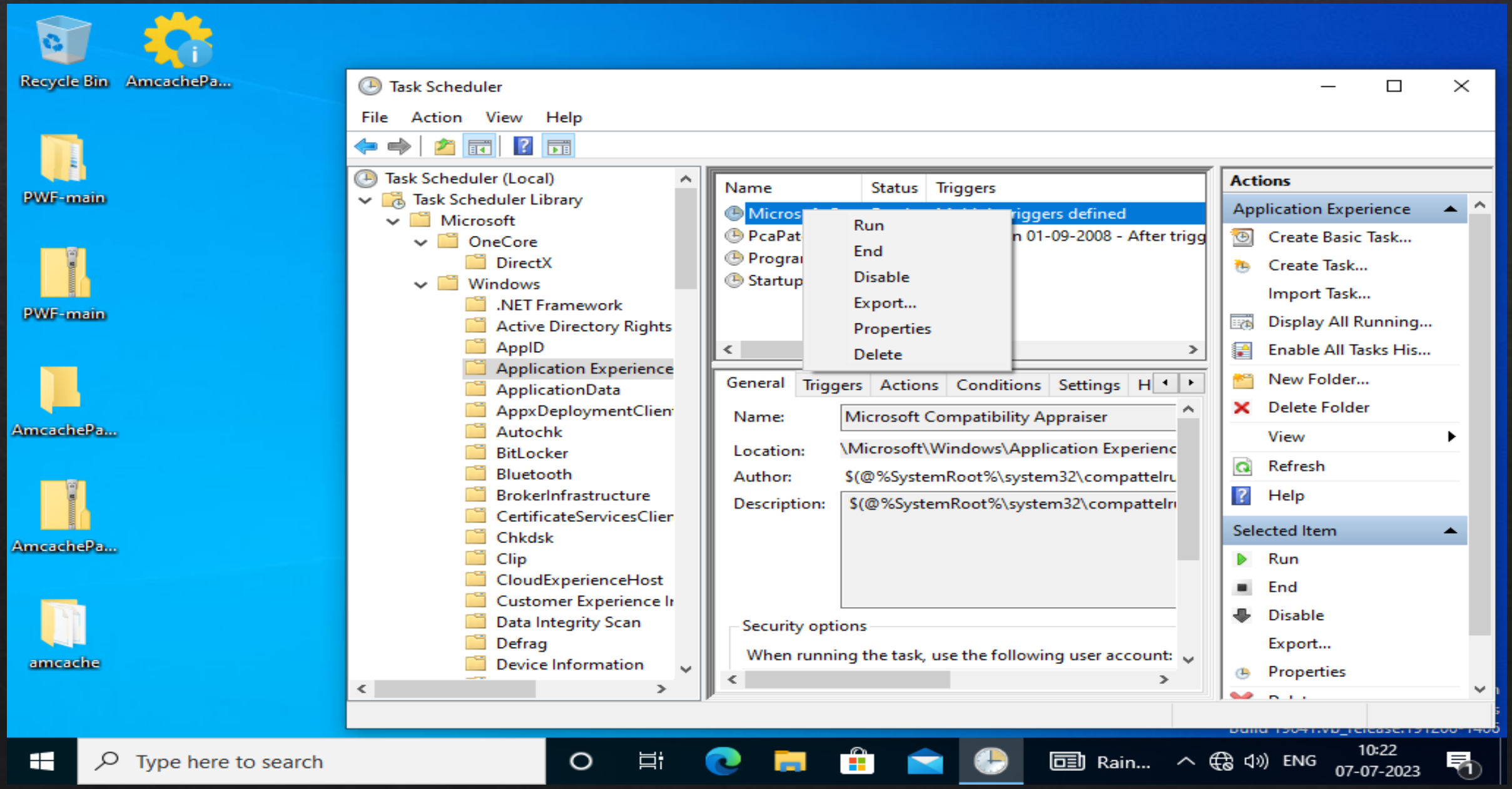
All File create in Amcache folder. Amcache folder copy the main pc and open with excel and show the output.

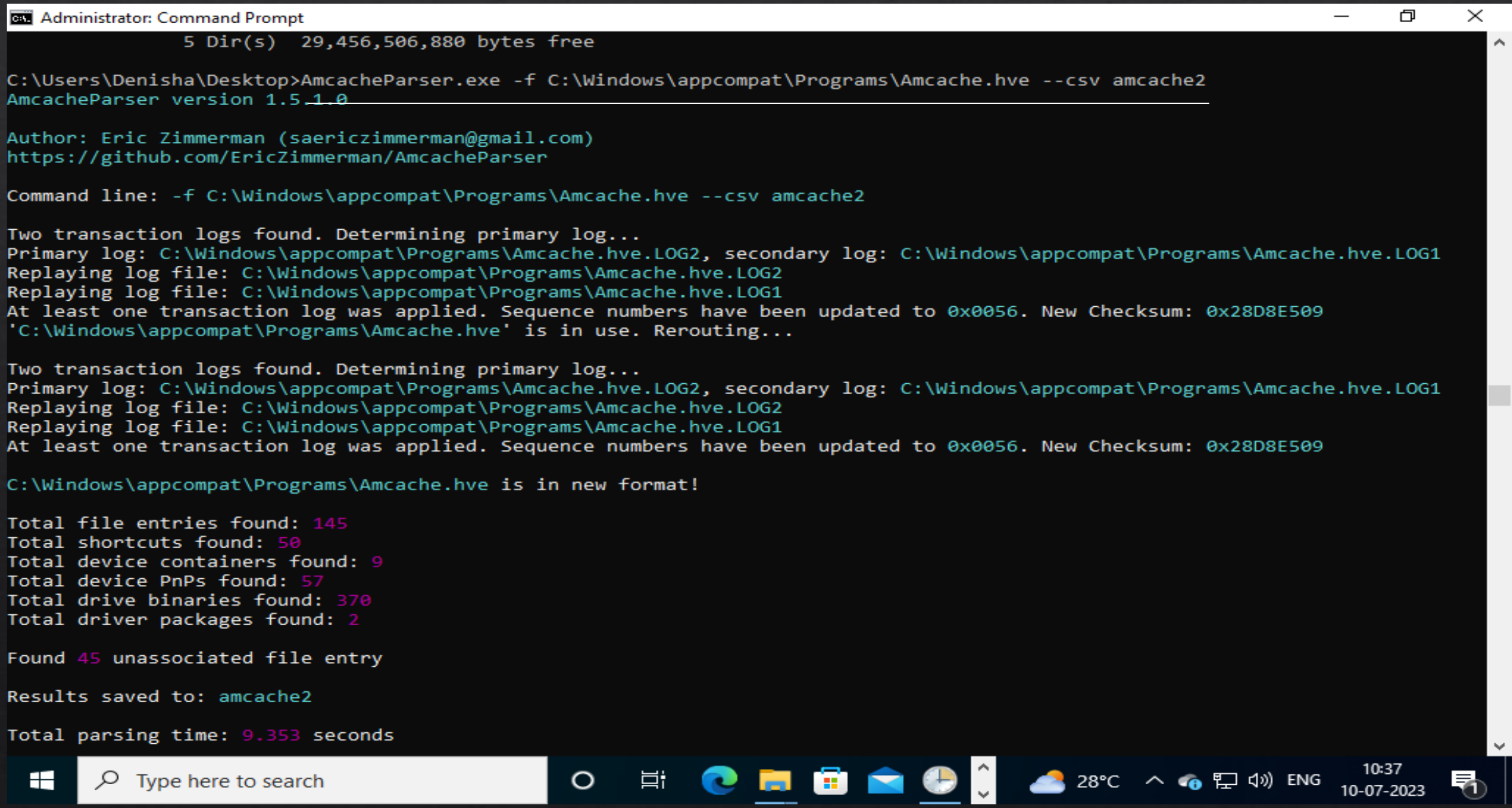


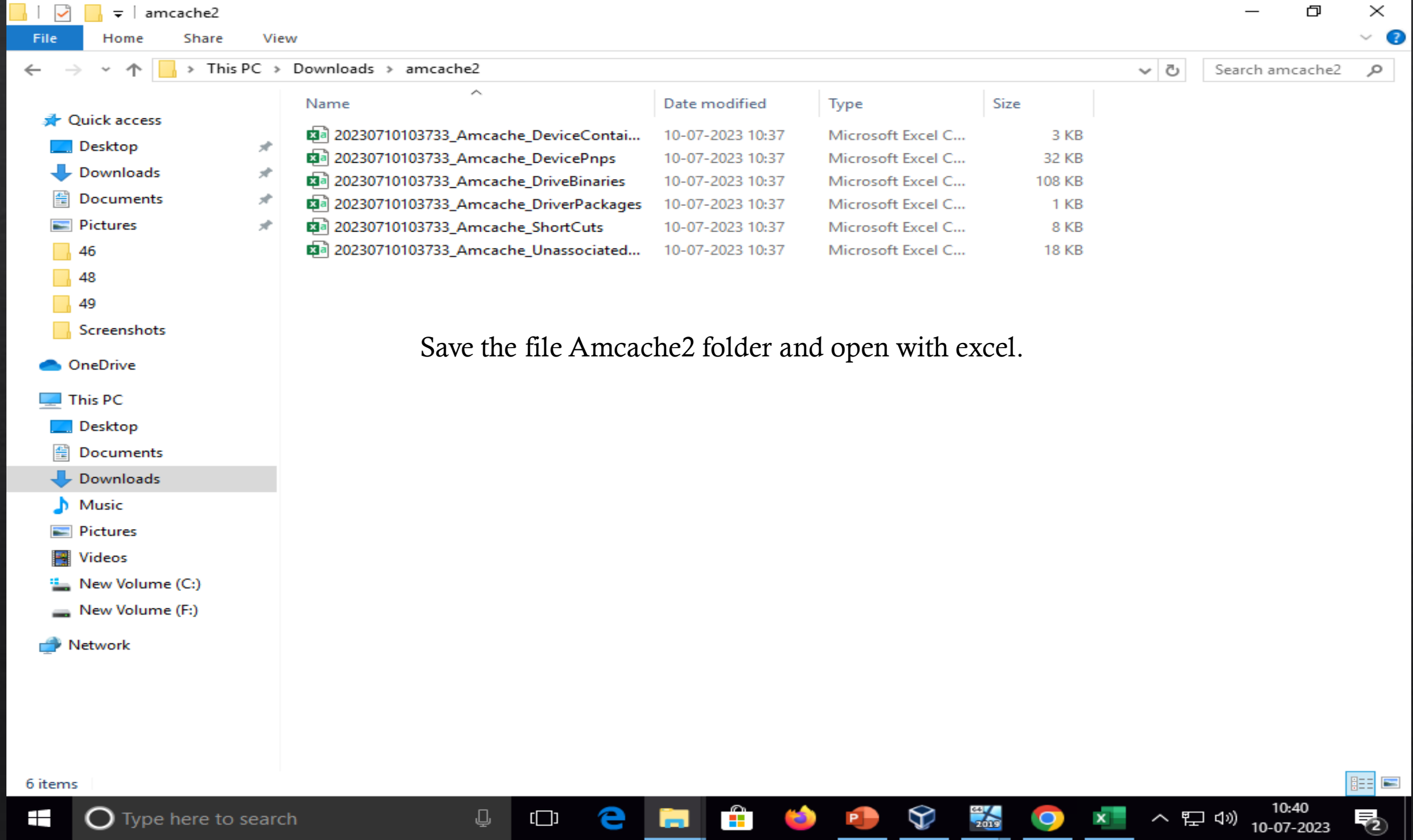

amcache
File
Home
Share
View
This PC
Downloads
amcache
Search amcache
Quick access
Desktop
Downloads
Documents
Pictures
46
48
49
Screenshots
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
New Volume (C:)
New Volume (F:)
Network
Name
Date modified
Type
Size
20230706214236_Amcache_DeviceContai...
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
All file shown in main pc and open with excel.
6 items
1 item selected 14.0 KB
Type here to search
10:30
10-07-2023

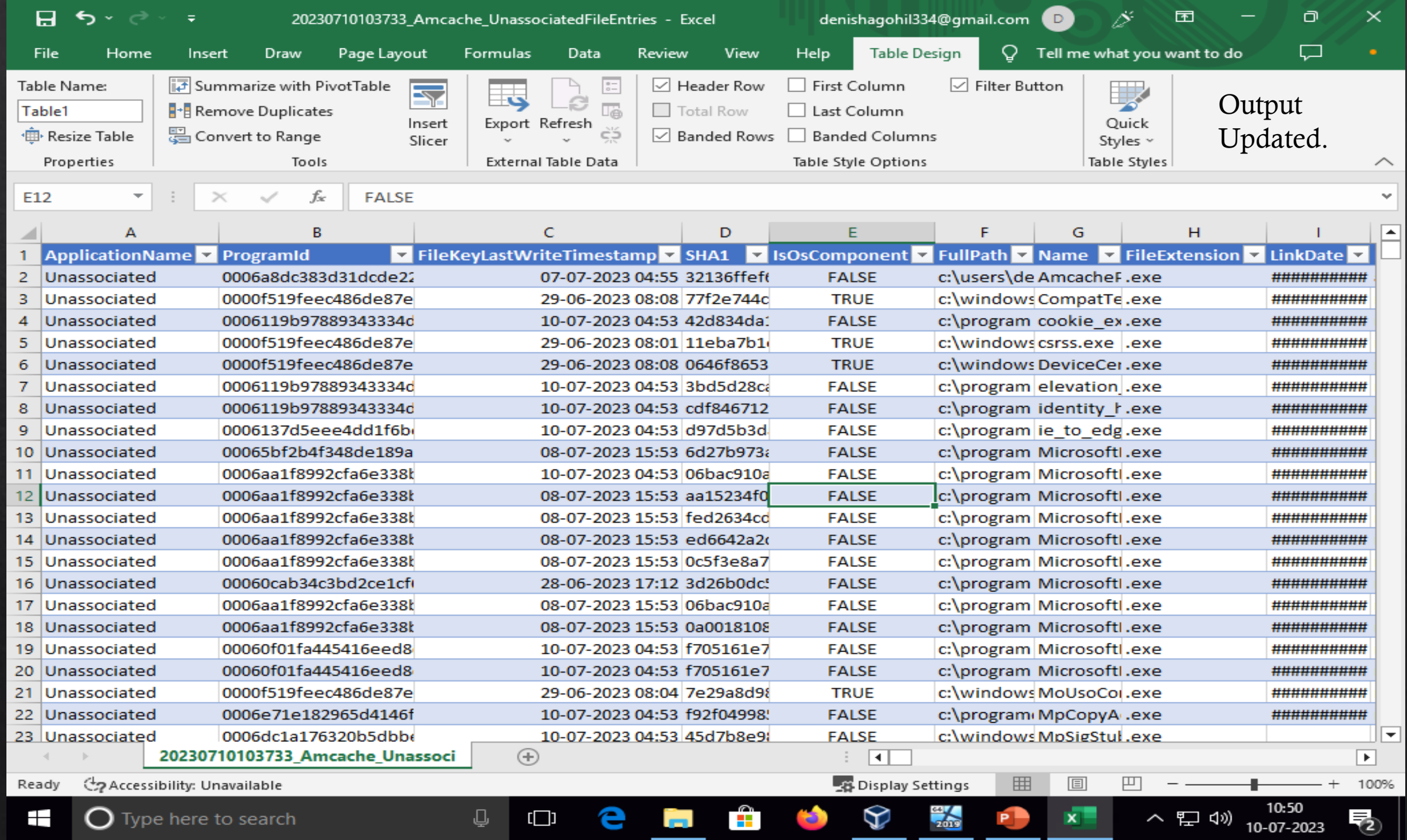

20230706214236_Amcache_UnassociatedFileEntries - Excel
Table Tools
Sign in
File Home Insert Draw Page Layout Formulas Data Review View Help Table Design
Tell me what you want to do
Table Name:
Table1
Resize Table
Properties
Summarize with PivotTable
Remove Duplicates
Convert to Range
Tools
Insert Slicer
Export
Refresh
External Table Data
Header Row
Total Row
Banded Rows
First Column
Last Column
Banded Columns
Filter Button
Table Style Options
Quick Styles
Table Styles
Amcache Entry
A5
Unassociated
Column16364 ProgramId FileKeyLastWriteTimestamp SHA1 IsOsComponent FullPath Name FileExtension LinkDate
Unassociated 0006a8dc383c 05-07-2023 08:39 32136ffef FALSE c:\users\de AmcacheF .exe 24-10-2052 08:04
Unassociated 0000f519feec 29-06-2023 08:08 77f2e744c TRUE c:\windows CompatTe .exe 18-10-2025 04:45
Unassociated 0006f3904a4b 29-06-2023 08:09 074349c30 FALSE c:\program cookie_ex .exe 21-06-2023 22:30
Unassociated 0000f519feec 29-06-2023 08:01 11eba7b1 TRUE c:\windows csrss.exe .exe 25-05-1971 13:07
Unassociated 0000f519feec 29-06-2023 08:08 0646f8653 TRUE c:\windows DeviceCer .exe 19-05-2039 12:13
Unassociated 0006f3904a4b 29-06-2023 08:09 777ac620a FALSE c:\program elevation_ .exe 21-06-2023 22:30
Unassociated 0006f3904a4b 29-06-2023 08:09 872cc644f FALSE c:\program identity_h .exe 21-06-2023 22:30
Unassociated 0006e0870de2 29-06-2023 08:09 5dedd60f7 FALSE c:\program ie_to_edg .exe 21-06-2023 22:30
Unassociated 0006ae478658 29-06-2023 08:09 690897252 FALSE c:\program Microsoft .exe 06-06-2023 18:16
Unassociated 0006868509b0 29-06-2023 08:09 7f6daa619 FALSE c:\program Microsoft .exe 06-06-2023 18:15
Unassociated 0006868509b0 29-06-2023 08:09 076f72b14 FALSE c:\program Microsoft .exe 06-06-2023 18:16
Unassociated 0006868509b0 29-06-2023 08:09 9f5c3fd02 FALSE c:\program Microsoft .exe 06-06-2023 18:22
Unassociated 0006868509b0 29-06-2023 08:09 9f5c3fd02 FALSE c:\program Microsoft .exe 06-06-2023 18:22
Unassociated 00060cab34c3 28-06-2023 17:12 3d26b0dc5 FALSE c:\program Microsoft .exe 22-07-2021 01:16
Unassociated 0006868509b0 29-06-2023 08:09 b61a5756c FALSE c:\program Microsoft .exe 06-06-2023 18:16
Unassociated 0006868509b0 29-06-2023 08:09 7f7c48ad1 FALSE c:\program Microsoft .exe 06-06-2023 18:16
Unassociated 0006868509b0 29-06-2023 08:09 cc92d47f7 FALSE c:\program Microsoft .exe 06-06-2023 18:15
Unassociated 000651e5db32 29-06-2023 08:09 7c51ea622 FALSE c:\program Microsoft .exe 21-06-2023 22:30
Unassociated 000651e5db32 29-06-2023 08:09 7c51ea622 FALSE c:\program Microsoft .exe 21-06-2023 22:30
Unassociated 0000f519feec 29-06-2023 08:04 7e29a8d98 TRUE c:\windows MoUsoCor .exe 01-05-2068 18:03
Unassociated 0006f3904a4b 29-06-2023 08:09 fea1f23ec FALSE c:\program msedge.e .exe 21-06-2023 22:30
Unassociated 0006707b1ec4 29-06-2023 08:09 92332ecf2 FALSE c:\program msedgew .exe 21-06-2023 22:30
20230706214236_Amcache_Unassoci
Ready
Accessibility: Unavailable
Display Settings
100%
Type here to search
10:29
10-07-2023

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




Administrator: Command Prompt
5 Dir(s) 29,456,506,880 bytes free
C:\Users\Denisha\Desktop>AmcacheParser.exe -f C:\Windows\appcompat\Programs\Amcache.hve --csv amcache2
AmcacheParser version 1.5.1.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AmcacheParser
Command line: -f C:\Windows\appcompat\Programs\Amcache.hve --csv amcache2
Two transaction logs found. Determining primary log...
Primary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG2, secondary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG1
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1
At least one transaction log was applied. Sequence numbers have been updated to 0x0056. New Checksum: 0x28D8E509
'C:\Windows\appcompat\Programs\Amcache.hve' is in use. Rerouting...
Two transaction logs found. Determining primary log...
Primary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG2, secondary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG1
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1
At least one transaction log was applied. Sequence numbers have been updated to 0x0056. New Checksum: 0x28D8E509
C:\Windows\appcompat\Programs\Amcache.hve is in new format!
Total file entries found: 145
Total shortcuts found: 50
Total device containers found: 9
Total device PnPs found: 57
Total drive binaries found: 370
Total driver packages found: 2
Found 45 unassociated file entry
Results saved to: amcache2
Total parsing time: 9.353 seconds
Type here to search
28°C
ENG
10:37
10-07-2023

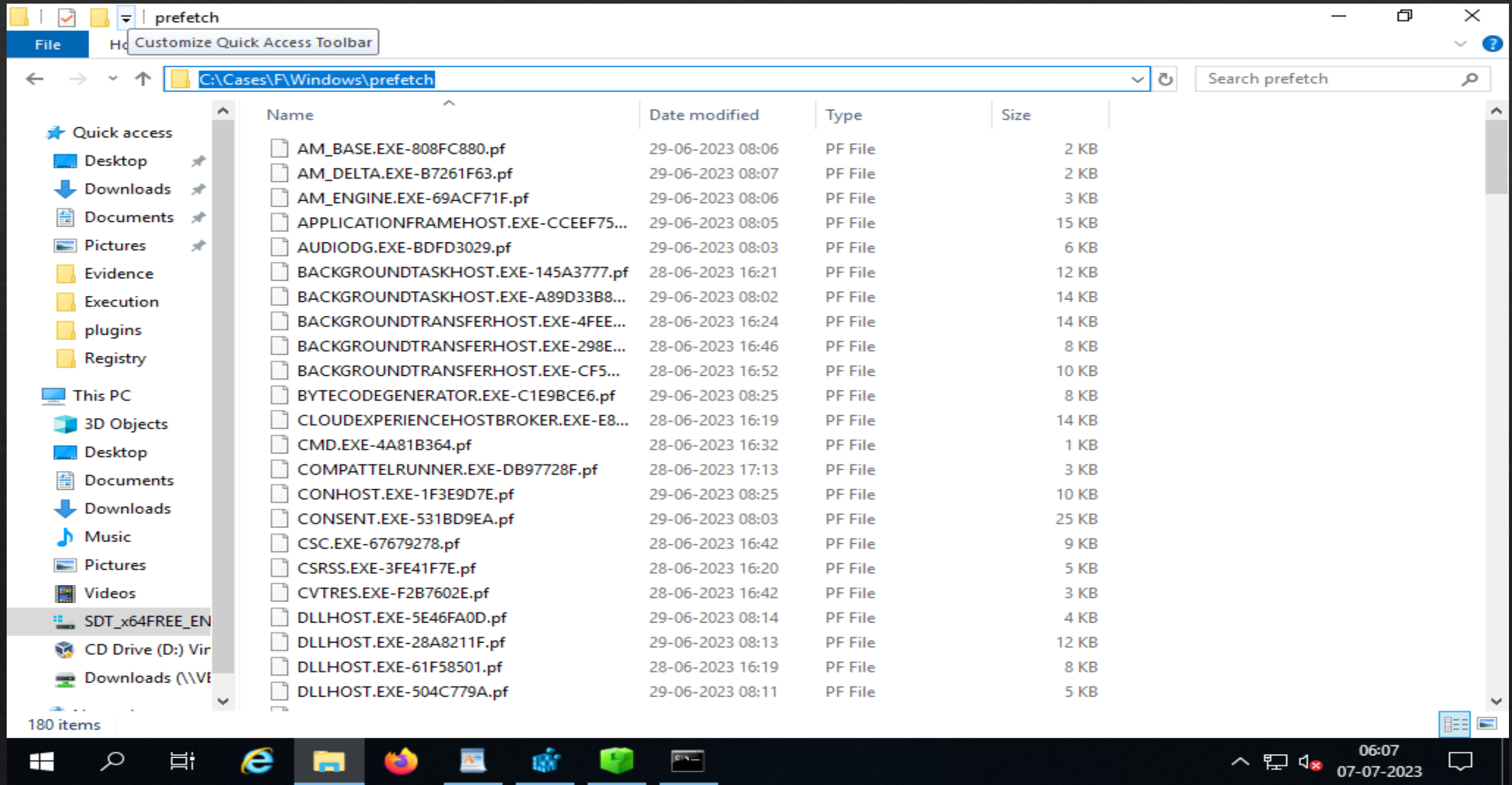

amcache2
File
Home
Share
View
This PC
Downloads
amcache2
Search amcache2
Quick access
Desktop
Downloads
Documents
Pictures
46
48
49
Screenshots
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
New Volume (C:)
New Volume (F:)
Network
Name
Date modified
Type
Size
20230710103733_Amcache_DeviceContai...
10-07-2023 10:37
Microsoft Excel C...
3 KB
20230710103733_Amcache_DevicePnps
10-07-2023 10:37
Microsoft Excel C...
32 KB
20230710103733_Amcache_DriveBinaries
10-07-2023 10:37
Microsoft Excel C...
108 KB
20230710103733_Amcache_DriverPackages
10-07-2023 10:37
Microsoft Excel C...
1 KB
20230710103733_Amcache_ShortCuts
10-07-2023 10:37
Microsoft Excel C...
8 KB
20230710103733_Amcache_Unassociated...
10-07-2023 10:37
Microsoft Excel C...
18 KB
Save the file Amcache2 folder and open with excel.
6 items
Type here to search
10:40
10-07-2023


20230710103733_Amcache_UnassociatedFileEntries - Excel
denishagohil334@gmail.com
File Home Insert Draw Page Layout Formulas Data Review View Help Table Design Tell me what you want to do
Table Name: Table1
Resize Table
Properties
Summarize with PivotTable
Remove Duplicates
Convert to Range
Tools
Insert Slicer
Export Refresh
External Table Data
Header Row
Total Row
Banded Rows
First Column
Last Column
Banded Columns
Filter Button
Table Style Options
Quick Styles
Table Styles
Output Updated.
E12
FALSE
A ApplicationName
B ProgramId
C FileKeyLastWriteTimestamp
D SHA1
E IsOsComponent
F FullPath
G Name
H FileExtension
I 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 42d834da1 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 Microsoft .exe ##########
11 Unassociated 0006aa1f8992cfa6e338 10-07-2023 04:53 06bac910a FALSE c:\program Microsoft .exe ##########
12 Unassociated 0006aa1f8992cfa6e338 08-07-2023 15:53 aa15234f0 FALSE c:\program Microsoft .exe ##########
13 Unassociated 0006aa1f8992cfa6e338 08-07-2023 15:53 fed2634cd FALSE c:\program Microsoft .exe ##########
14 Unassociated 0006aa1f8992cfa6e338 08-07-2023 15:53 ed6642a2c FALSE c:\program Microsoft .exe ##########
15 Unassociated 0006aa1f8992cfa6e338 08-07-2023 15:53 0c5f3e8a7 FALSE c:\program Microsoft .exe ##########
16 Unassociated 00060cab34c3bd2ce1cf 28-06-2023 17:12 3d26b0dc5 FALSE c:\program Microsoft .exe ##########
17 Unassociated 0006aa1f8992cfa6e338 08-07-2023 15:53 06bac910a FALSE c:\program Microsoft .exe ##########
18 Unassociated 0006aa1f8992cfa6e338 08-07-2023 15:53 0a0018108 FALSE c:\program Microsoft .exe ##########
19 Unassociated 00060f01fa445416eed8 10-07-2023 04:53 f705161e7 FALSE c:\program Microsoft .exe ##########
20 Unassociated 00060f01fa445416eed8 10-07-2023 04:53 f705161e7 FALSE c:\program Microsoft .exe ##########
21 Unassociated 0000f519feec486de87e 29-06-2023 08:04 7e29a8d98 TRUE c:\windows MoUsoCor .exe ##########
22 Unassociated 0006e71e182965d4146f 10-07-2023 04:53 f92f04998 FALSE c:\program MpCopyA .exe ##########
23 Unassociated 0006dc1a176320b5dbbe 10-07-2023 04:53 45d7b8e9 FALSE c:\windows MpSigStub .exe
20230710103733_Amcache_Unassoci
Ready
Accessibility: Unavailable
Display Settings
100%
Type here to search
10:50
10-07-2023

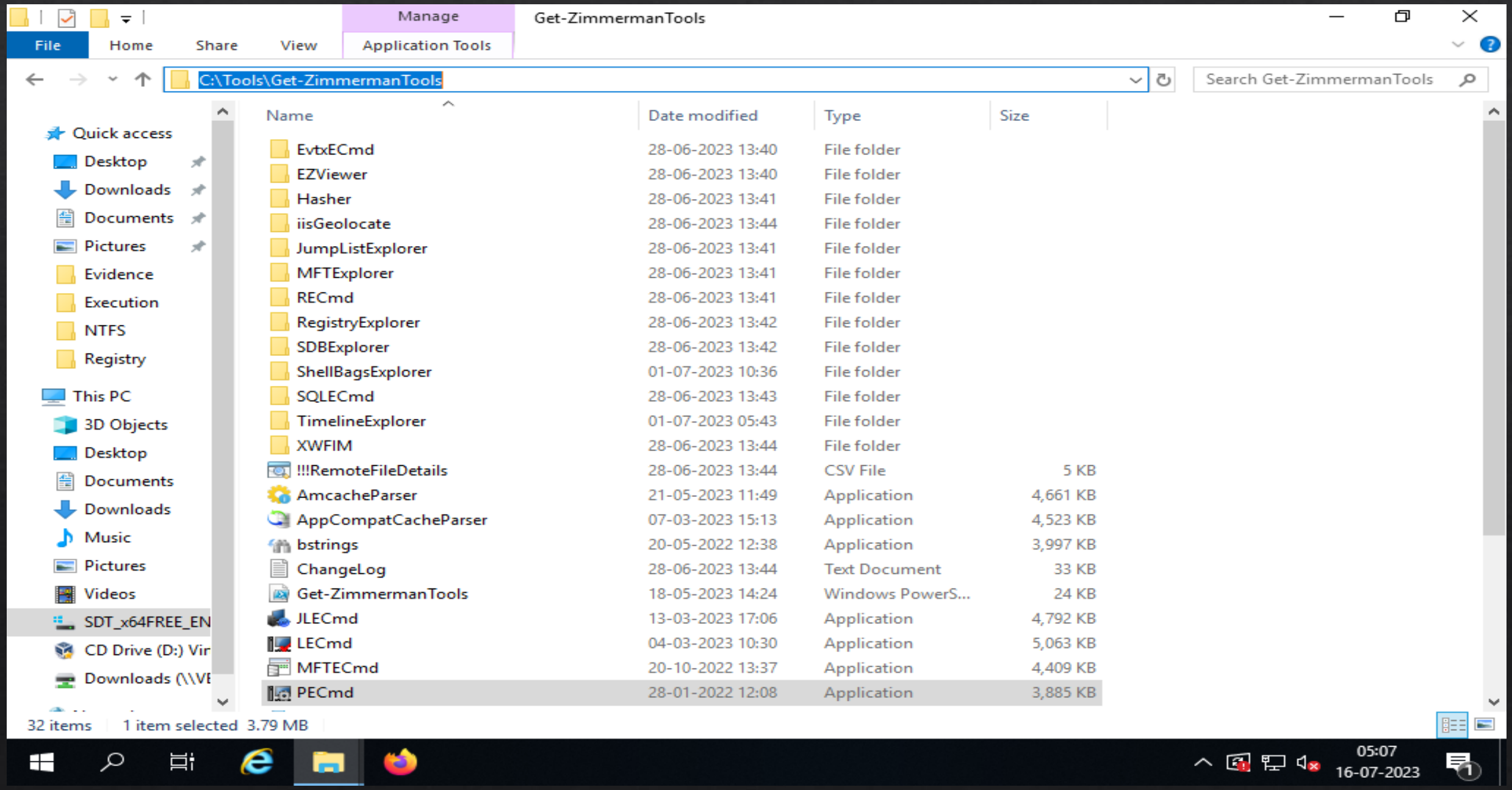
4. Windows Prefetch Analysis

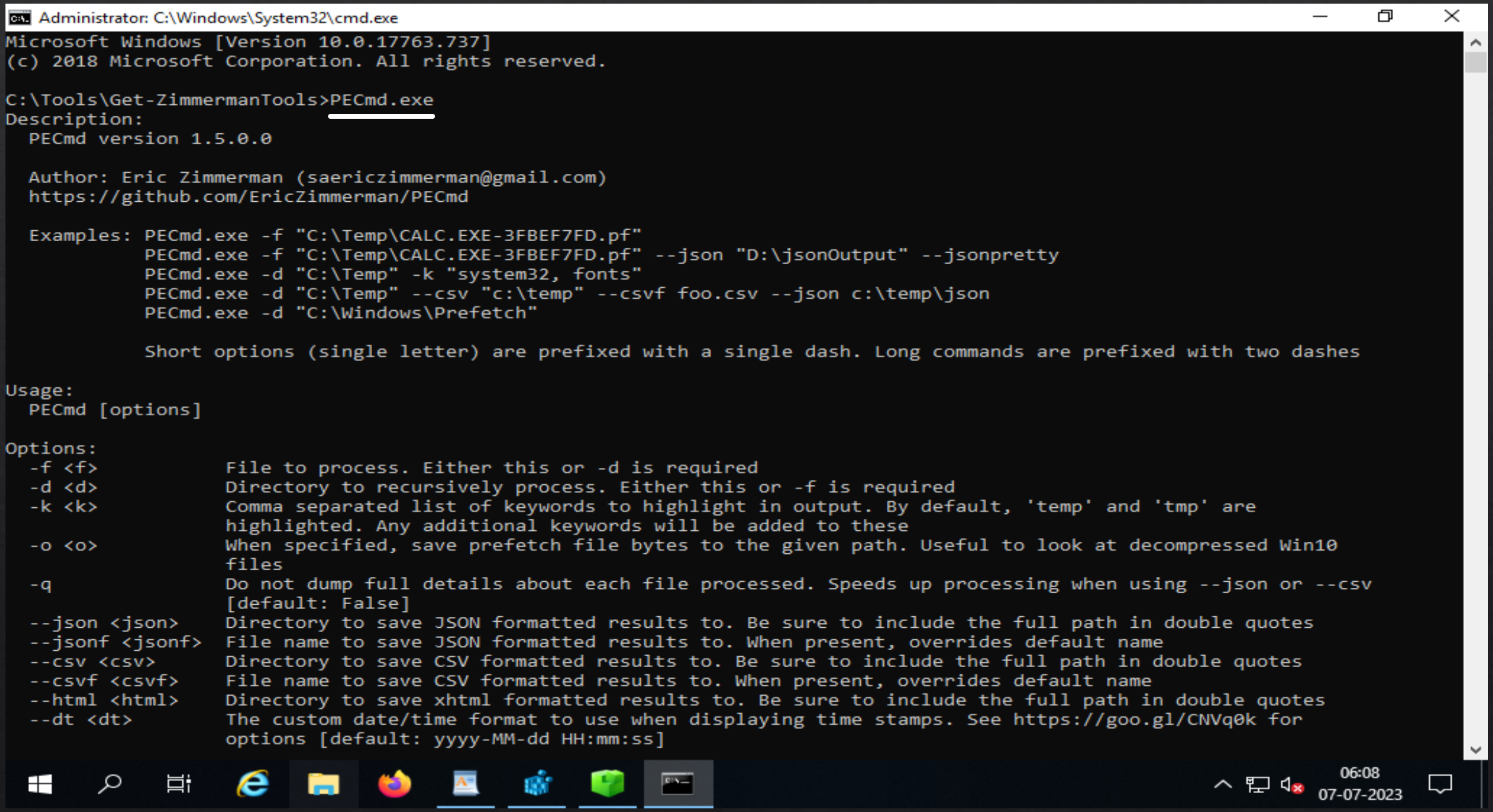
Accessing Prefetch Files for Forensic Analysis. A digital forensic investigation often aims to determine the activities of a user on a computer. Prefetch files are an important type of evidence, which provide detailed information about the programs that were run on a computer.

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



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




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 https://goo.gl/CNVq0k for options [default: yyyy-MM-dd HH:mm:ss]
06:08
07-07-2023

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

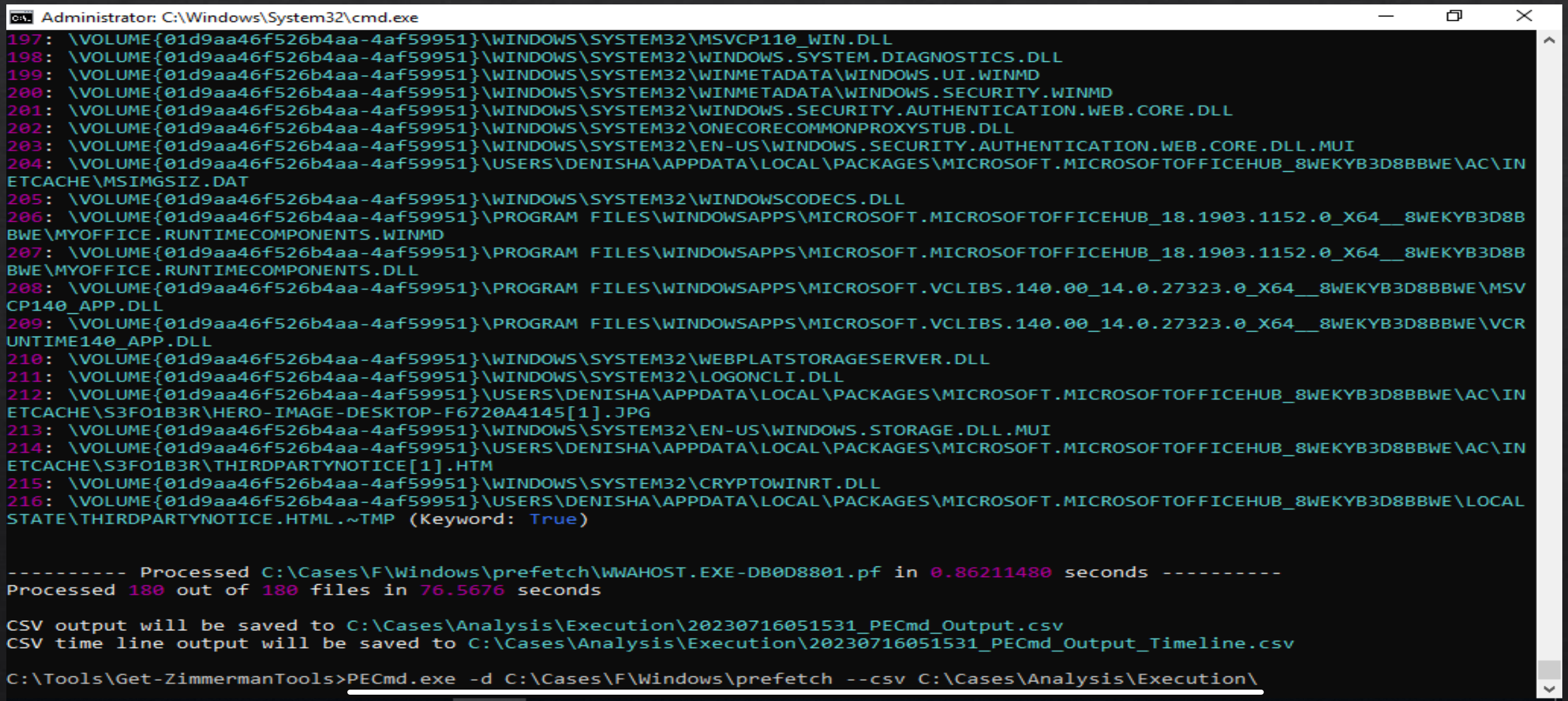
```
Either -f or -d is required. Exiting

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

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

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

Keywords: temp, tmp

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

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

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

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

Volume information:

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

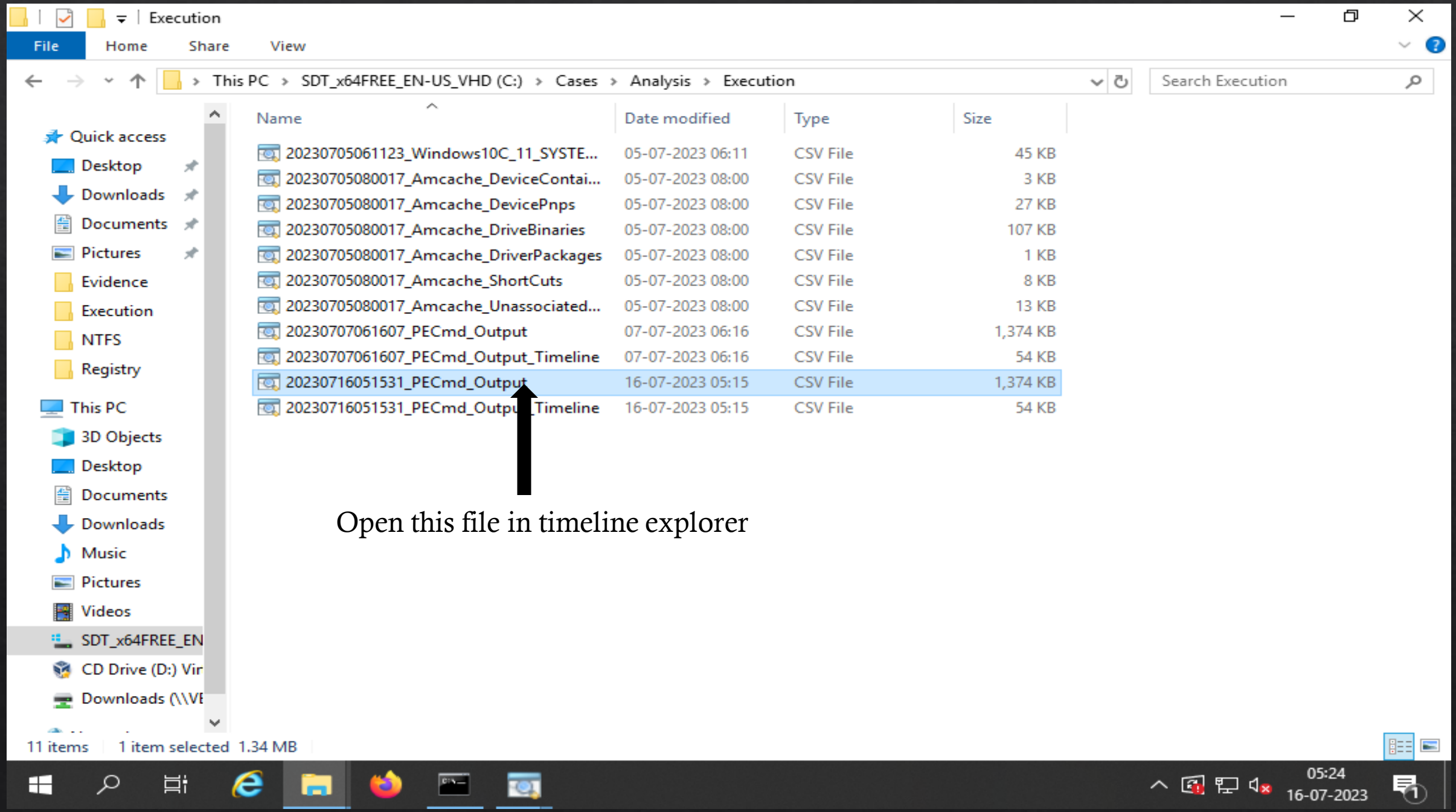
Administrator: C:\Windows\System32\cmd.exe

```
06

Directories referenced: 20

00: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES
01: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS
02: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_NEUTRAL_SPLIT.SCALE-100_8WEKYB3D8BBWE
03: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_NEUTRAL_SPLIT.SCALE-100_8WEKYB3D8BBWE\IMAGES
04: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_X64__8WEKYB3D8BBWE
05: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_X64__8WEKYB3D8BBWE\MICROSOFT.SYSTEM.PACKAGE.METADATA
06: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSSTORE_11910.1002.5.0_NEUTRAL_SPLIT.SCALE-100_8WEKYB3D8BBWE
07: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSSTORE_11910.1002.5.0_NEUTRAL_SPLIT.SCALE-100_8WEKYB3D8BBWE\ASSETS
08: \VOLUME{01d9aa46f526b4aa-4af59951}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWSSTORE_11910.1002.5.0_NEUTRAL_SPLIT.SCALE-100_8WEKYB3D8BBWE\ASSETS\APPTILES
09: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS
10: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\FONTS
11: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\GLOBALIZATION
12: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\GLOBALIZATION\SORTING
13: \VOLUME{01d9aa46f526b4aa-4af59951}\WINDOWS\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
```

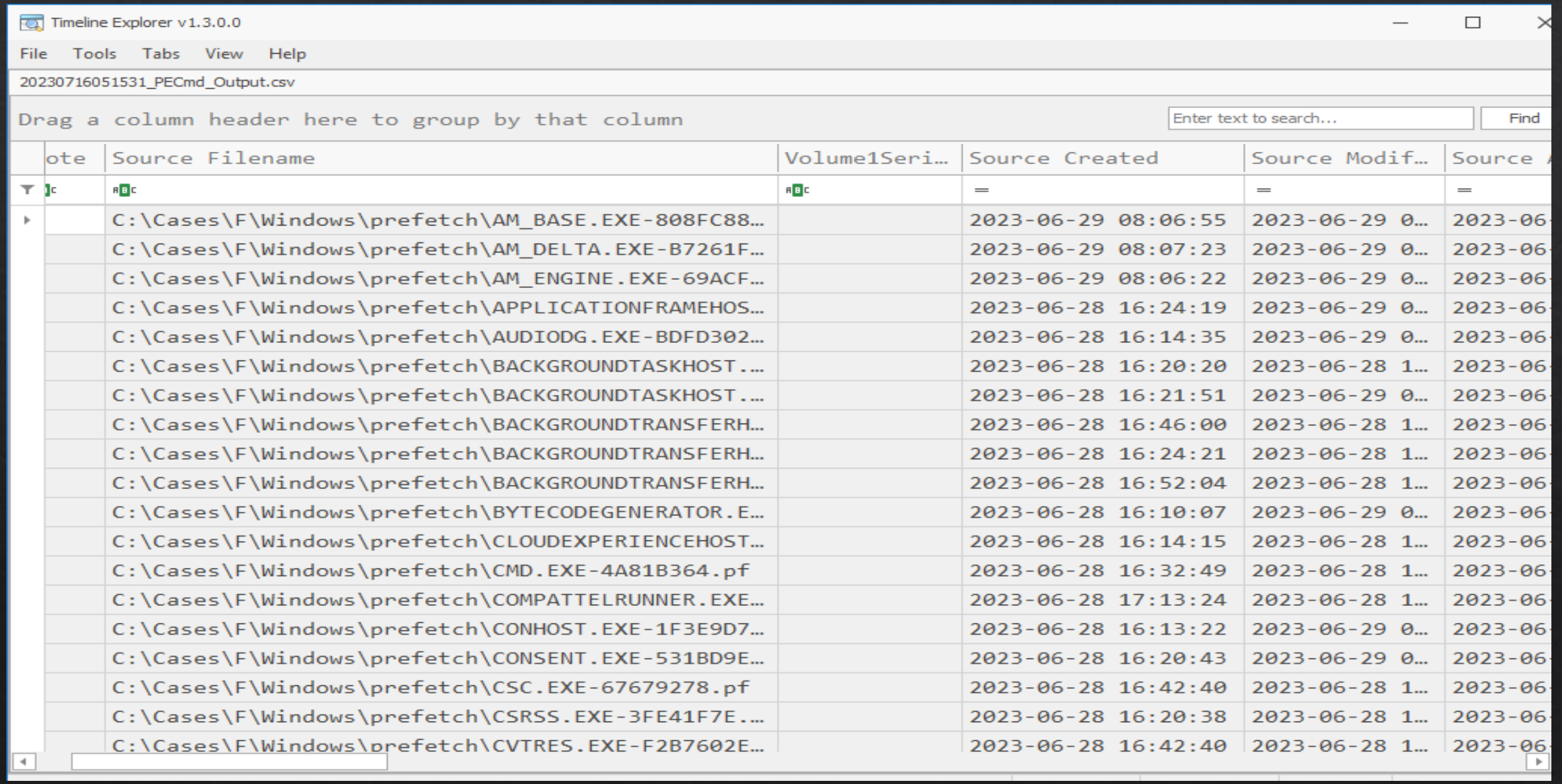
5. Windows Prefetch Timeline Analysis

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




Execution
File
Home
Share
View
This PC
SDT_x64FREE_EN-US_VHD (C:)
Cases
Analysis
Execution
Search Execution
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 (\\VE
Name
Date modified
Type
Size
20230705061123_Windows10C_11_SYSTE... 05-07-2023 06:11 CSV File 45 KB
20230705080017_Amcache_DeviceContai... 05-07-2023 08:00 CSV File 3 KB
20230705080017_Amcache_DevicePnps 05-07-2023 08:00 CSV File 27 KB
20230705080017_Amcache_DriveBinaries 05-07-2023 08:00 CSV File 107 KB
20230705080017_Amcache_DriverPackages 05-07-2023 08:00 CSV File 1 KB
20230705080017_Amcache_ShortCuts 05-07-2023 08:00 CSV File 8 KB
20230705080017_Amcache_Unassociated... 05-07-2023 08:00 CSV File 13 KB
20230707061607_PECmd_Output 07-07-2023 06:16 CSV File 1,374 KB
20230707061607_PECmd_Output_Timeline 07-07-2023 06:16 CSV File 54 KB
20230716051531_PECmd_Output 16-07-2023 05:15 CSV File 1,374 KB
20230716051531_PECmd_Output_Timeline 16-07-2023 05:15 CSV File 54 KB
Open this file in timeline explorer
11 items
1 item selected 1.34 MB
05:24
16-07-2023

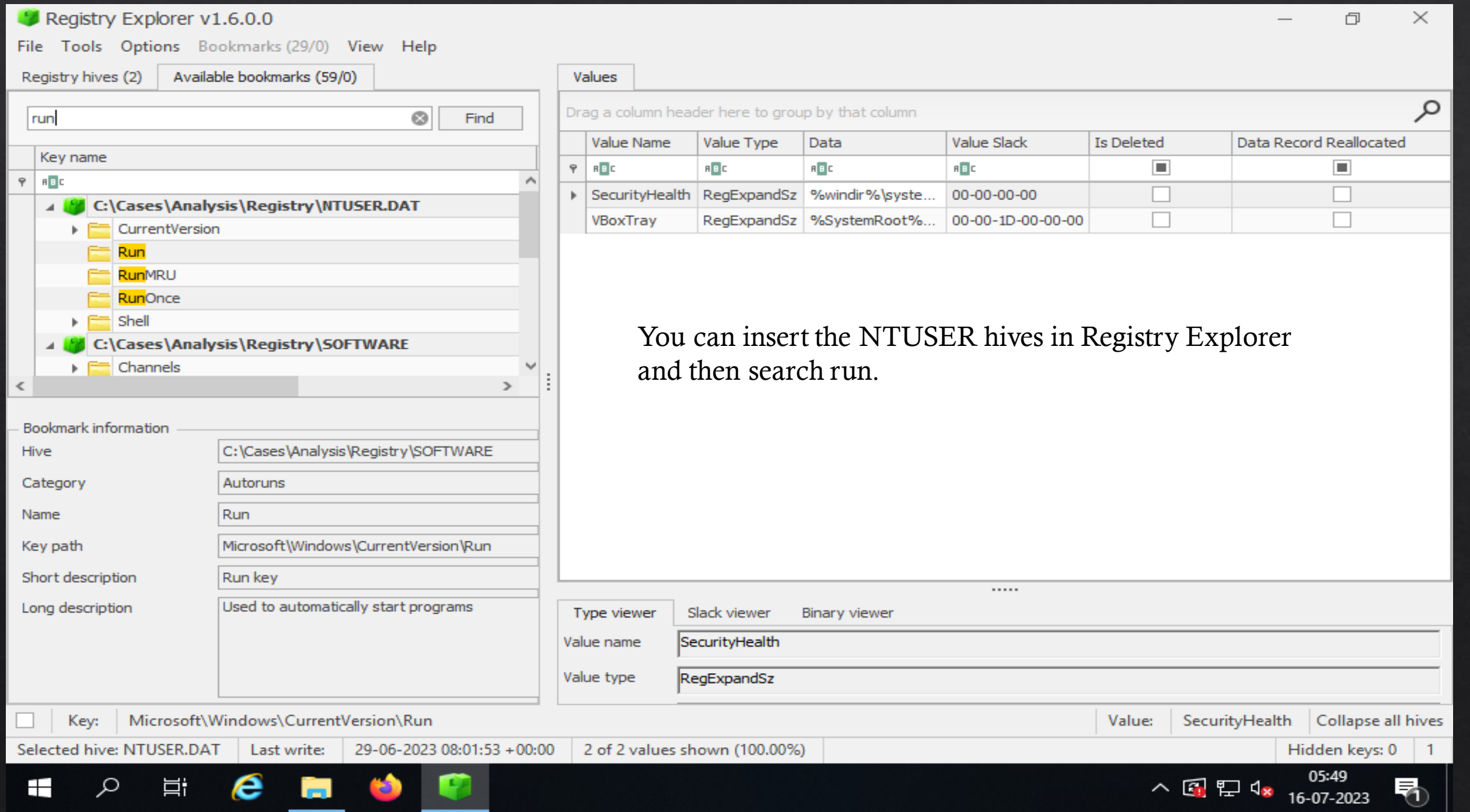
Show the All prefetch file with time

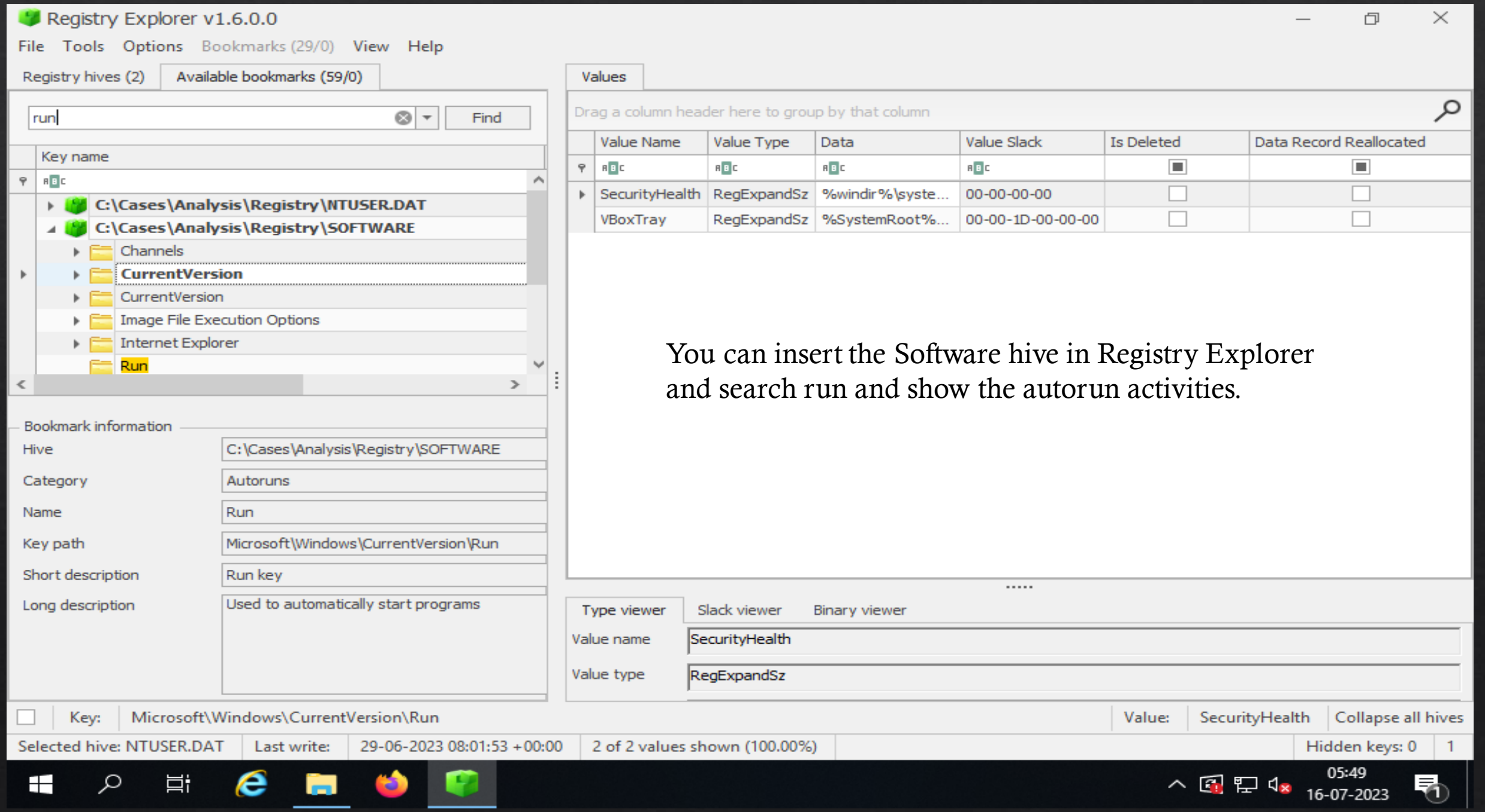


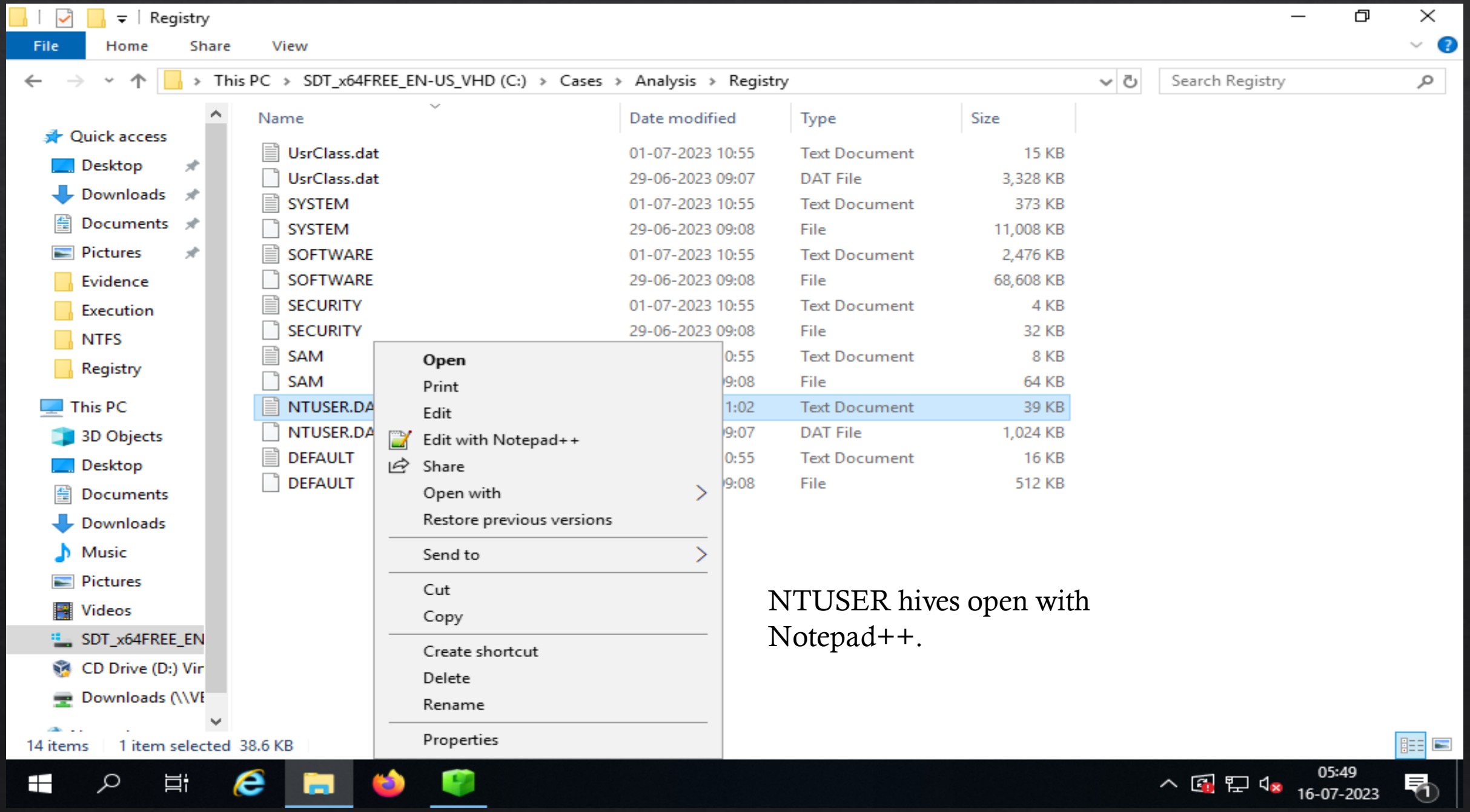
ote	Source Filename	Volume1Seri…	Source Created	Source Modif…	Source A
	C:\Cases\F\Windows\prefetch\AM_BASE.EXE-808FC88…		2023-06-29 08:06:55	2023-06-29 0…	2023-06
	C:\Cases\F\Windows\prefetch\AM_DELTA.EXE-B7261F…		2023-06-29 08:07:23	2023-06-29 0…	2023-06
	C:\Cases\F\Windows\prefetch\AM_ENGINE.EXE-69ACF…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

Auto run keys Analysis

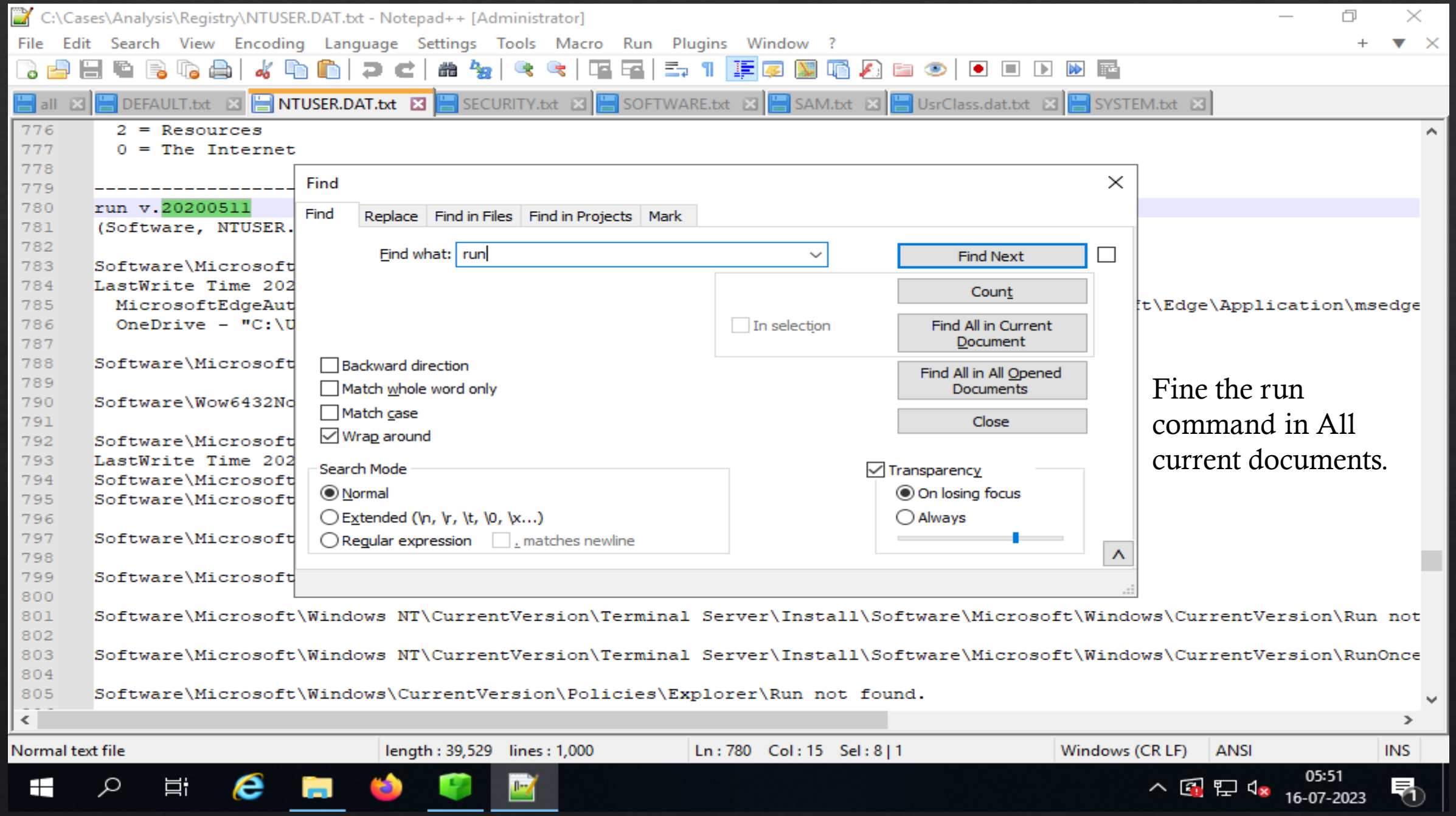
Autorun and run keys are registry entries that allow programs to execute automatically when a device is connected or a user logs on. Malicious actors can use them to launch malware, bypass security controls, and maintain persistence on compromised hosts.


Registry Explorer v1.6.0.0
File Tools Options Bookmarks (29/0) View Help
Registry hives (2) Available bookmarks (59/0)
run
Find
Key name
C:\Cases\Analysis\Registry\NTUSER.DAT
CurrentVersion
Run
RunMRU
RunOnce
Shell
C:\Cases\Analysis\Registry\SOFTWARE
Channels
Bookmark information
Hive C:\Cases\Analysis\Registry\SOFTWARE
Category Autoruns
Name Run
Key path Microsoft\Windows\CurrentVersion\Run
Short description Run key
Long description Used to automatically start programs
Values
Drag a column header here to group by that column
Value Name
Value Type
Data
Value Slack
Is Deleted
Data Record Reallocated
SecurityHealth RegExpandSz %windir%\syste... 00-00-00-00
VBoxTray RegExpandSz %SystemRoot%... 00-00-1D-00-00-00
You can insert the NTUSER hives in Registry Explorer and then search run.
Type viewer
Slack viewer
Binary viewer
Value name SecurityHealth
Value type RegExpandSz
Key: Microsoft\Windows\CurrentVersion\Run
Value: SecurityHealth
Collapse all hives
Selected hive: NTUSER.DAT
Last write: 29-06-2023 08:01:53 +00:00
2 of 2 values shown (100.00%)
Hidden keys: 0
1
05:49
16-07-2023

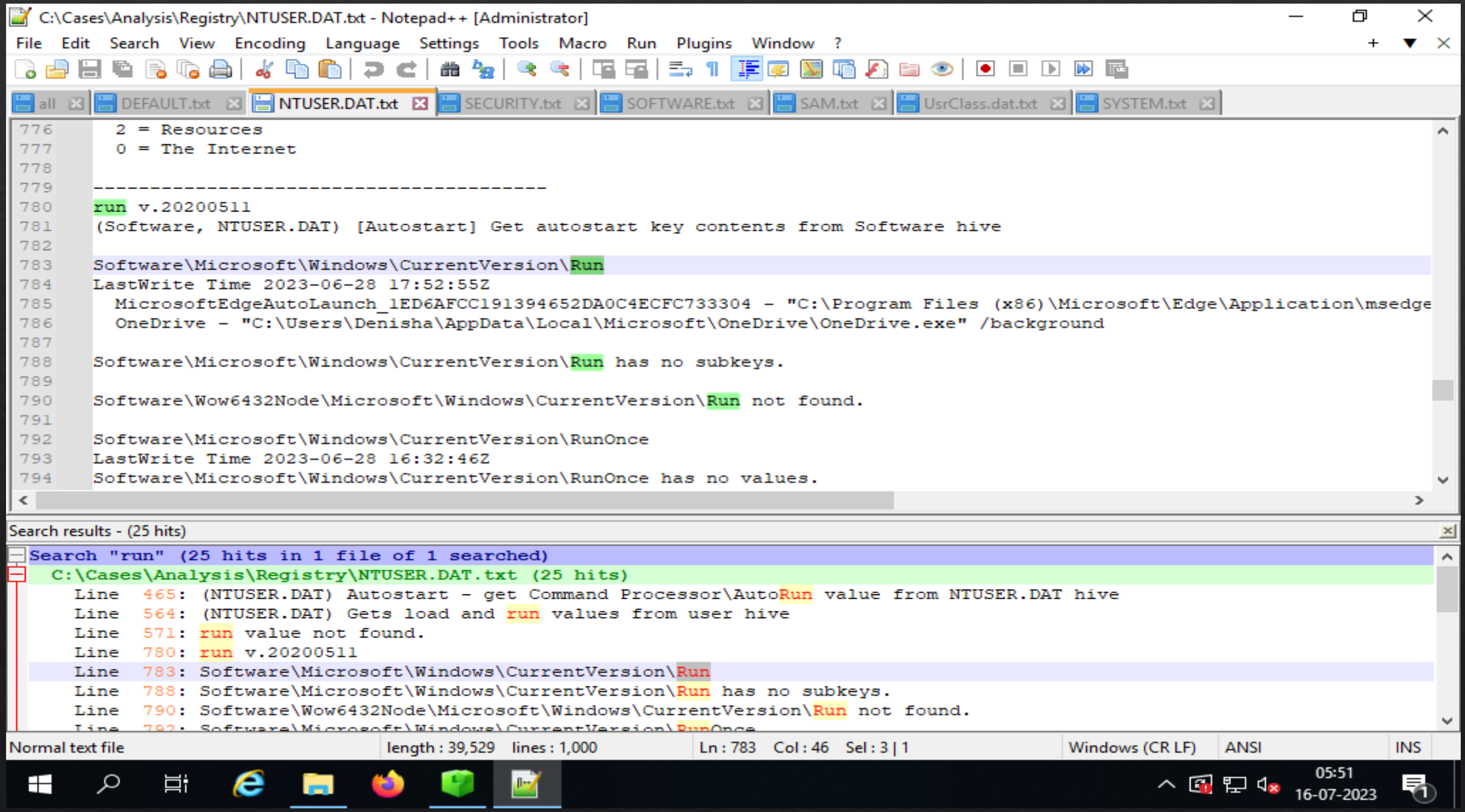

Registry Explorer v1.6.0.0
File Tools Options Bookmarks (29/0) View Help
Registry hives (2) Available bookmarks (59/0)
run
Find
Key name
C:\Cases\Analysis\Registry\NTUSER.DAT
C:\Cases\Analysis\Registry\SOFTWARE
Channels
CurrentVersion
CurrentVersion
Image File Execution Options
Internet Explorer
Run
Bookmark information
Hive C:\Cases\Analysis\Registry\SOFTWARE
Category Autoruns
Name Run
Key path Microsoft\Windows\CurrentVersion\Run
Short description Run key
Long description Used to automatically start programs
Values
Drag a column header here to group by that column
Value Name
Value Type
Data
Value Slack
Is Deleted
Data Record Reallocated
SecurityHealth RegExpandSz %windir%\syste... 00-00-00-00
VBoxTray RegExpandSz %SystemRoot%... 00-00-1D-00-00-00
You can insert the Software hive in Registry Explorer and search run and show the autorun activities.
Type viewer Slack viewer Binary viewer
Value name SecurityHealth
Value type RegExpandSz
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

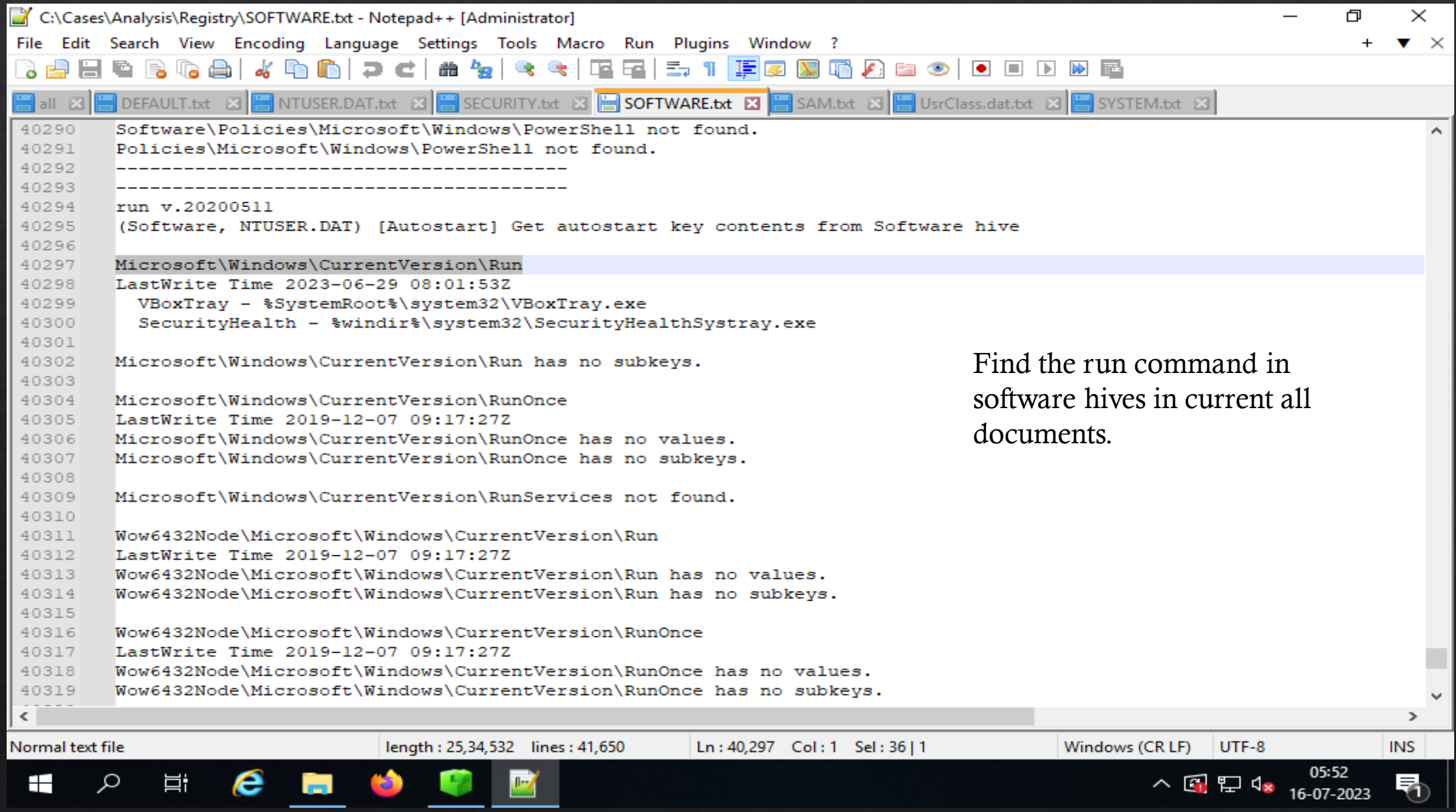


NTUSER hives open with Notepad++.



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
779 ----------
780 run v.20200511
781 (Software, NTUSER.DAT) [Autostart] Get autostart key contents from Software hive
782
783 Software\Microsoft\Windows\CurrentVersion\Run
784 LastWrite Time 2023-06-28 17:52:55Z
785 MicrosoftEdgeAutoLaunch_1ED6AFCC191394652DA0C4ECFC733304 - "C:\Program Files (x86)\Microsoft\Edge\Application\msedge
786 OneDrive - "C:\Users\Denisha\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
787
788 Software\Microsoft\Windows\CurrentVersion\Run has no subkeys.
789
790 Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.
791
792 Software\Microsoft\Windows\CurrentVersion\RunOnce
793 LastWrite Time 2023-06-28 16:32:46Z
794 Software\Microsoft\Windows\CurrentVersion\RunOnce has no values.
Search results - (25 hits)
Search "run" (25 hits in 1 file of 1 searched)
C:\Cases\Analysis\Registry\NTUSER.DAT.txt (25 hits)
Line 465: (NTUSER.DAT) Autostart - get Command Processor\AutoRun value from NTUSER.DAT hive
Line 564: (NTUSER.DAT) Gets load and run values from user hive
Line 571: run value not found.
Line 780: run v.20200511
Line 783: Software\Microsoft\Windows\CurrentVersion\Run
Line 788: Software\Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 790: Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.
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



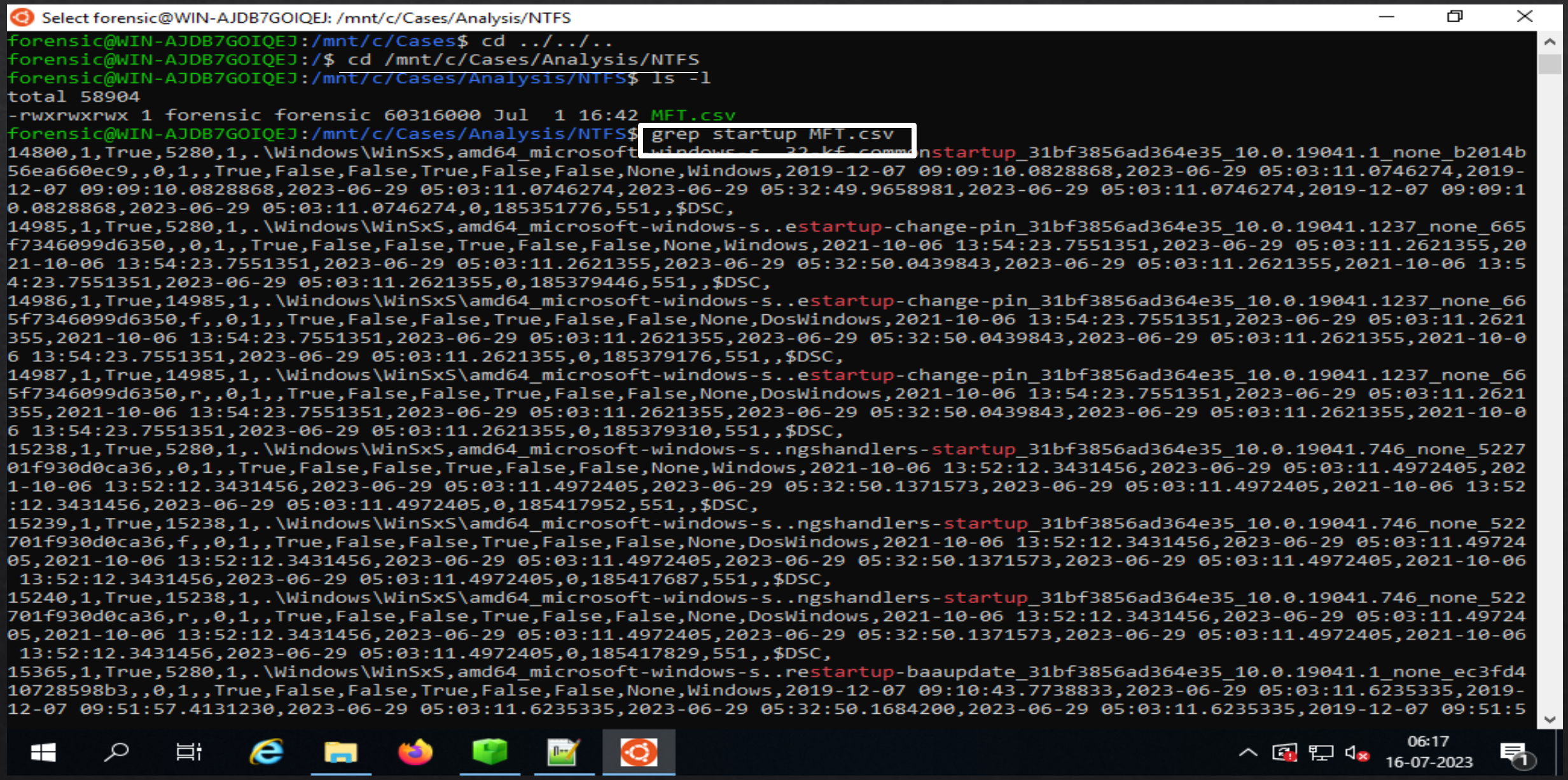
Find the run command in software hives in current all documents.

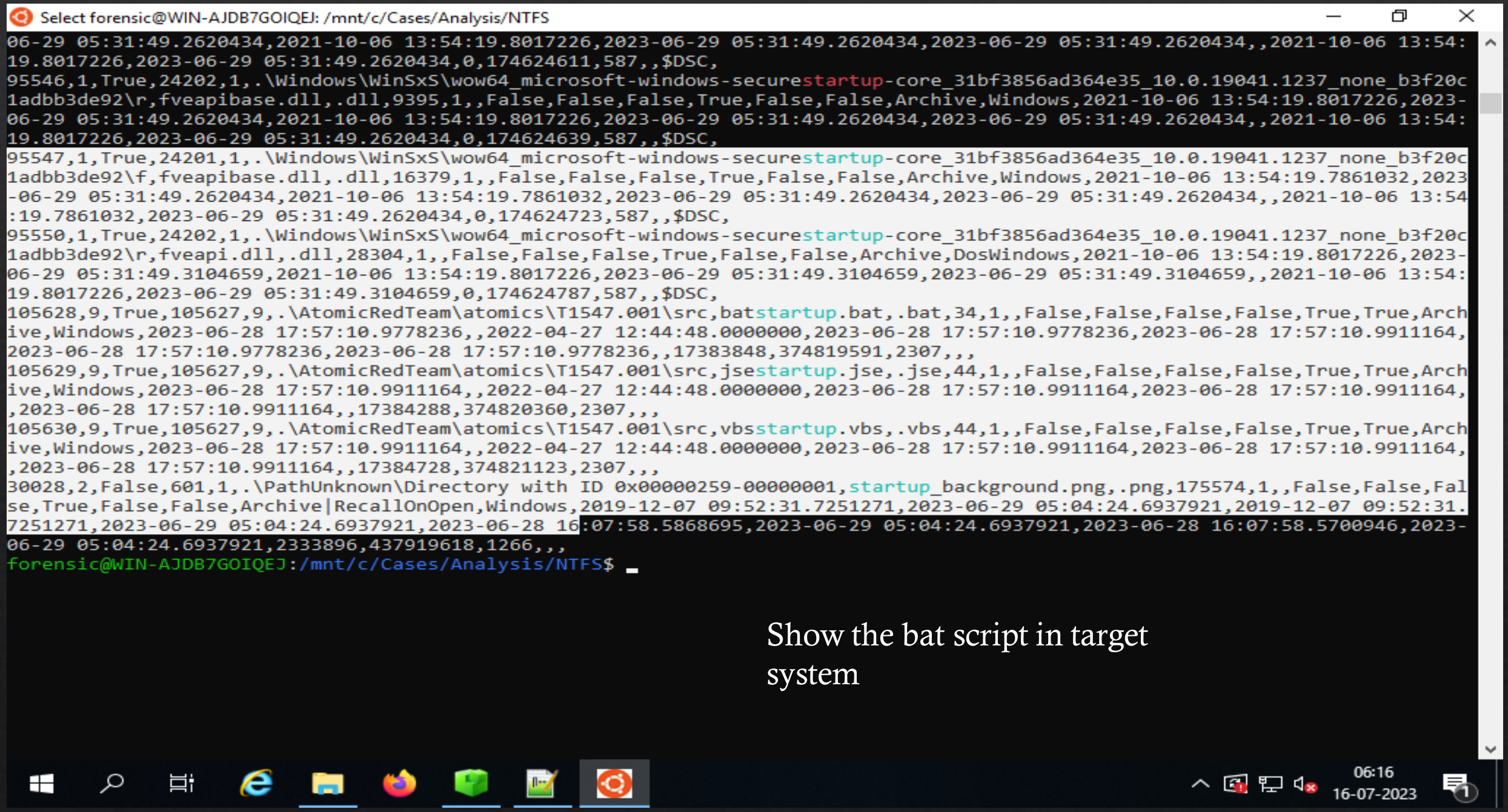
Startup Folder Analysis

Two location mention for startup folder.

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

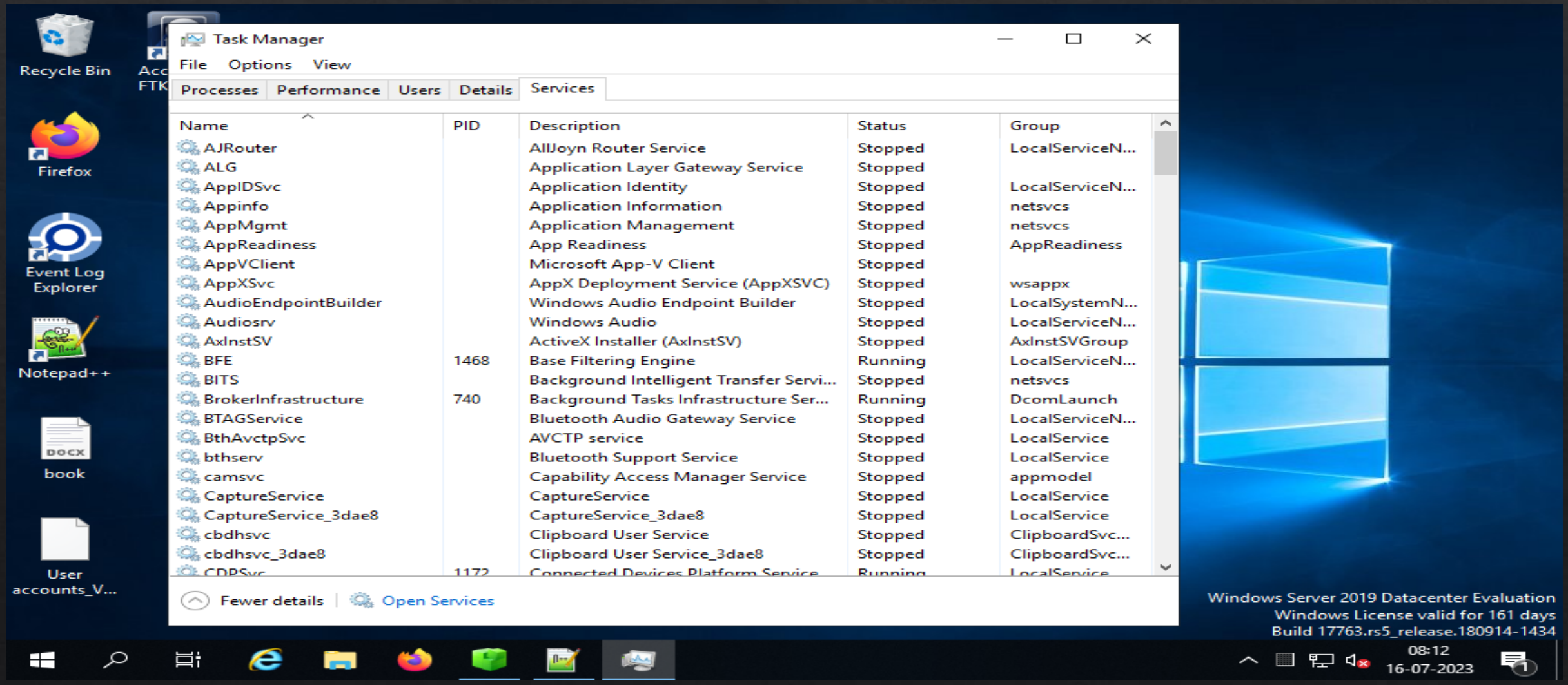
Open the given file location with ubuntu linux and use mnt directory , show mnt.csv file and using grep command show startup folders and scripts.

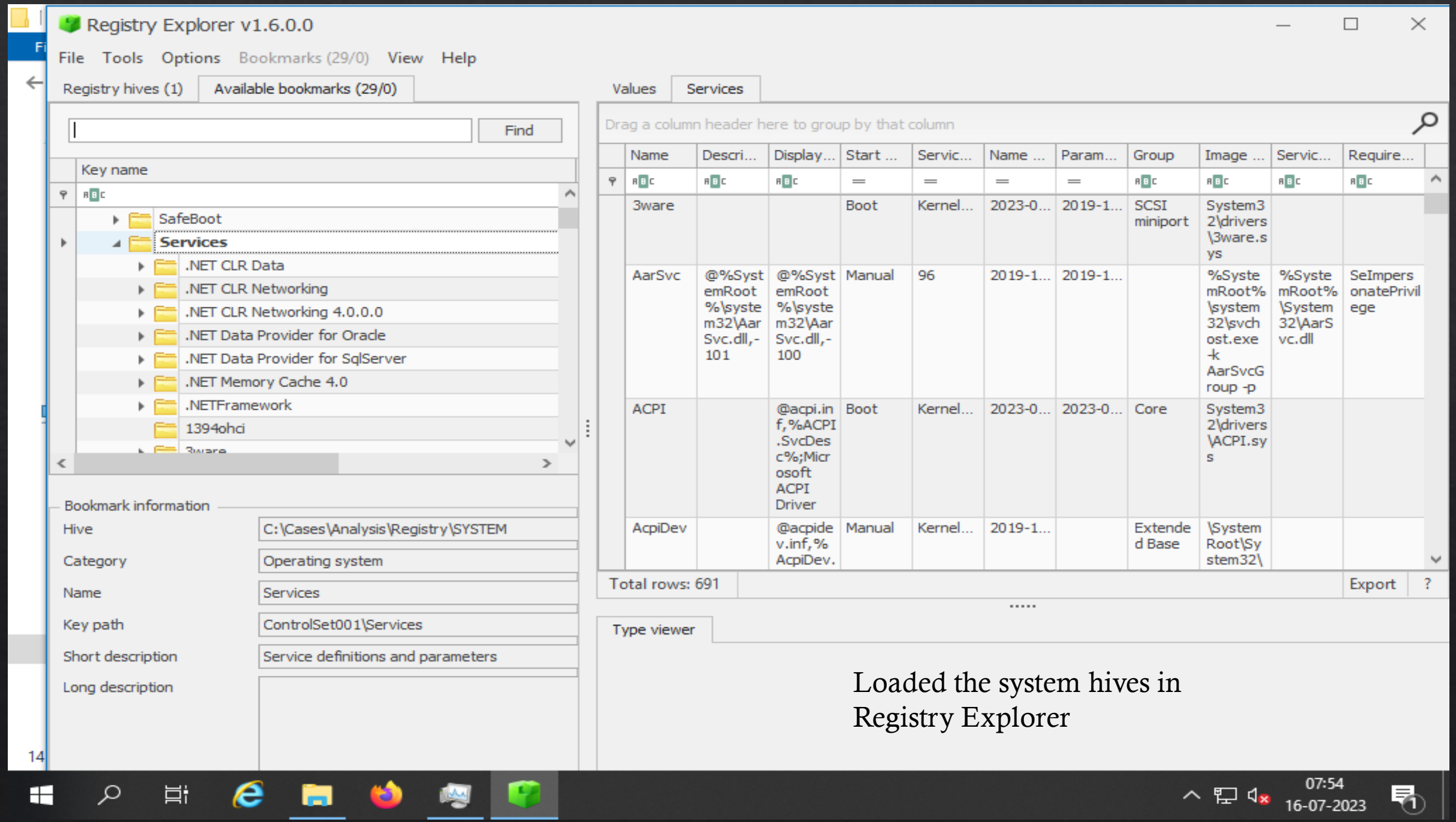


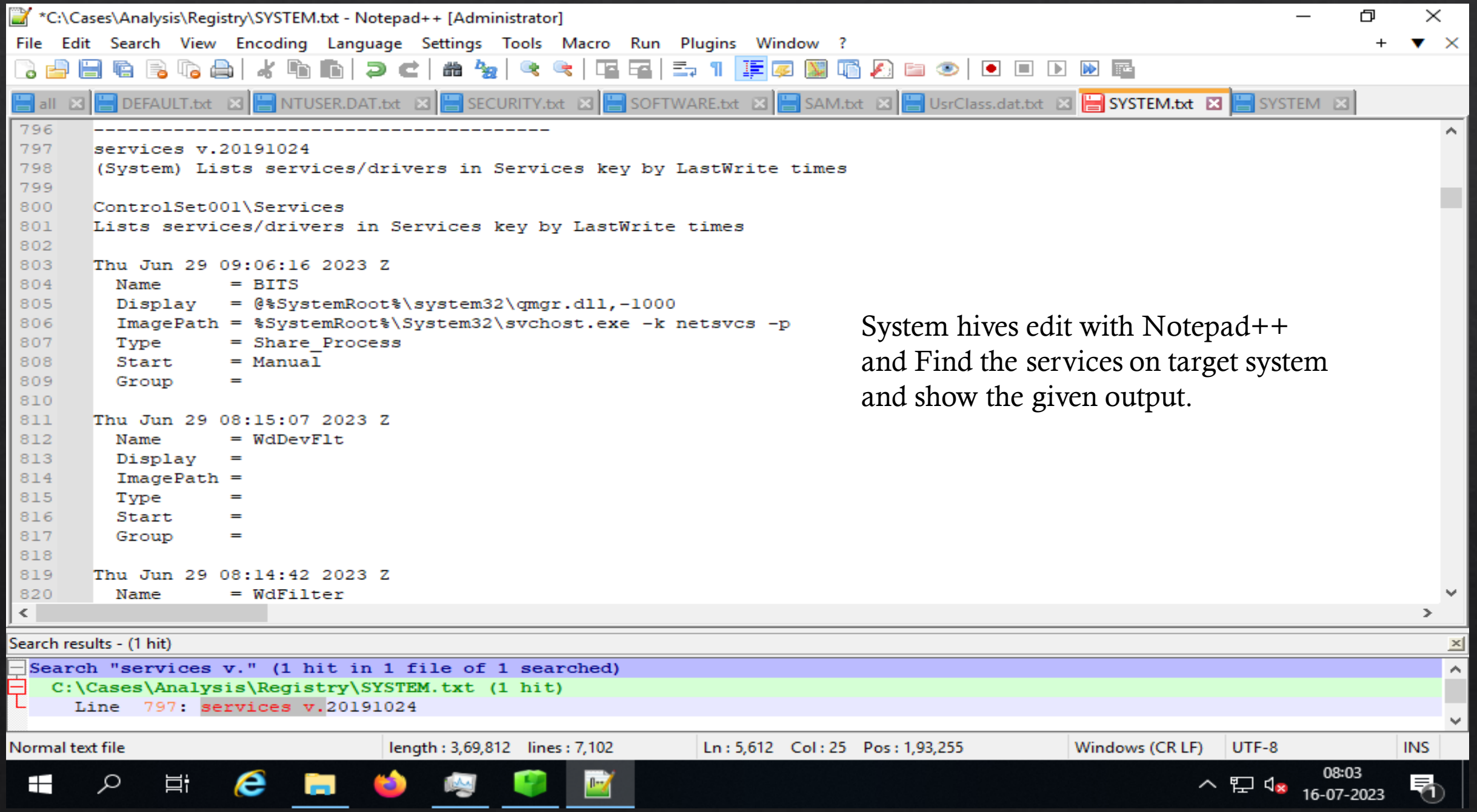

Select forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/NTFS
06-29 05:31:49.2620434,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.2620434,2023-06-29 05:31:49.2620434,,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.2620434,0,174624611,587,,$DSC,
95546,1,True,24202,1,.\Windows\WinSxS\wow64_microsoft-windows-securestartup-core_31bf3856ad364e35_10.0.19041.1237_none_b3f20c1adbb3de92\r,fveapibase.dll,.dll,9395,1,,False,False,False,True,False,False,Archive,Windows,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.2620434,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.2620434,2023-06-29 05:31:49.2620434,,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.2620434,0,174624639,587,,$DSC,
95547,1,True,24201,1,.\Windows\WinSxS\wow64_microsoft-windows-securestartup-core_31bf3856ad364e35_10.0.19041.1237_none_b3f20c1adbb3de92\f,fveapibase.dll,.dll,16379,1,,False,False,False,True,False,False,Archive,Windows,2021-10-06 13:54:19.7861032,2023-06-29 05:31:49.2620434,2021-10-06 13:54:19.7861032,2023-06-29 05:31:49.2620434,2023-06-29 05:31:49.2620434,,2021-10-06 13:54:19.7861032,2023-06-29 05:31:49.2620434,0,174624723,587,,$DSC,
95550,1,True,24202,1,.\Windows\WinSxS\wow64_microsoft-windows-securestartup-core_31bf3856ad364e35_10.0.19041.1237_none_b3f20c1adbb3de92\r,fveapi.dll,.dll,28304,1,,False,False,False,True,False,False,Archive,DosWindows,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.3104659,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.3104659,2023-06-29 05:31:49.3104659,,2021-10-06 13:54:19.8017226,2023-06-29 05:31:49.3104659,0,174624787,587,,$DSC,
105628,9,True,105627,9,.\AtomicRedTeam\atomics\T1547.001\src,batstartup.bat,.bat,34,1,,False,False,False,False,True,True,Archive,Windows,2023-06-28 17:57:10.9778236,,2022-04-27 12:44:48.0000000,2023-06-28 17:57:10.9778236,2023-06-28 17:57:10.9911164,2023-06-28 17:57:10.9778236,2023-06-28 17:57:10.9778236,,17383848,374819591,2307,,,
105629,9,True,105627,9,.\AtomicRedTeam\atomics\T1547.001\src,jsestartup.jse,.jse,44,1,,False,False,False,False,True,True,Archive,Windows,2023-06-28 17:57:10.9911164,,2022-04-27 12:44:48.0000000,2023-06-28 17:57:10.9911164,2023-06-28 17:57:10.9911164,,2023-06-28 17:57:10.9911164,,17384288,374820360,2307,,,
105630,9,True,105627,9,.\AtomicRedTeam\atomics\T1547.001\src,vbsstartup.vbs,.vbs,44,1,,False,False,False,False,True,True,Archive,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,False,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.

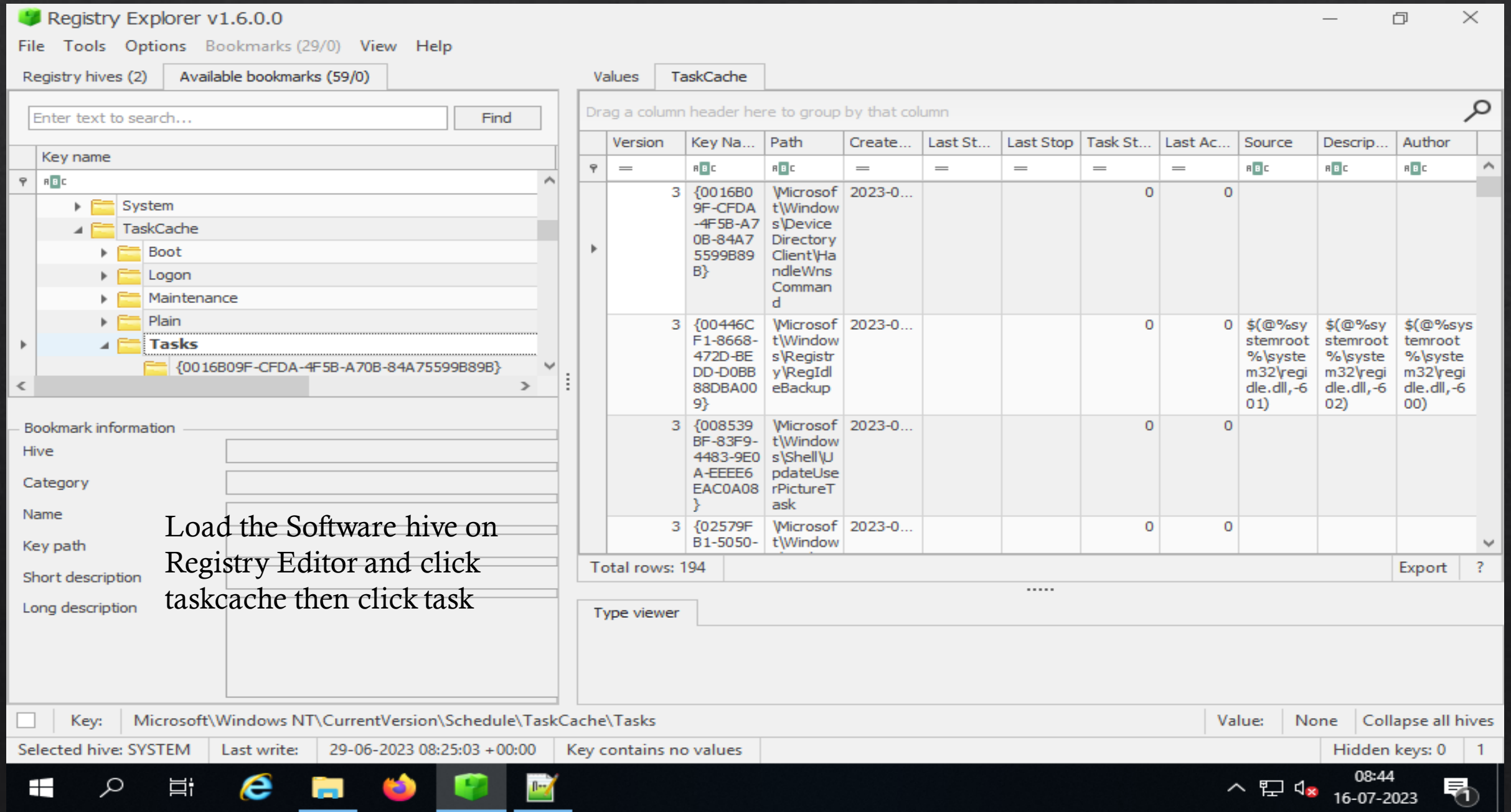


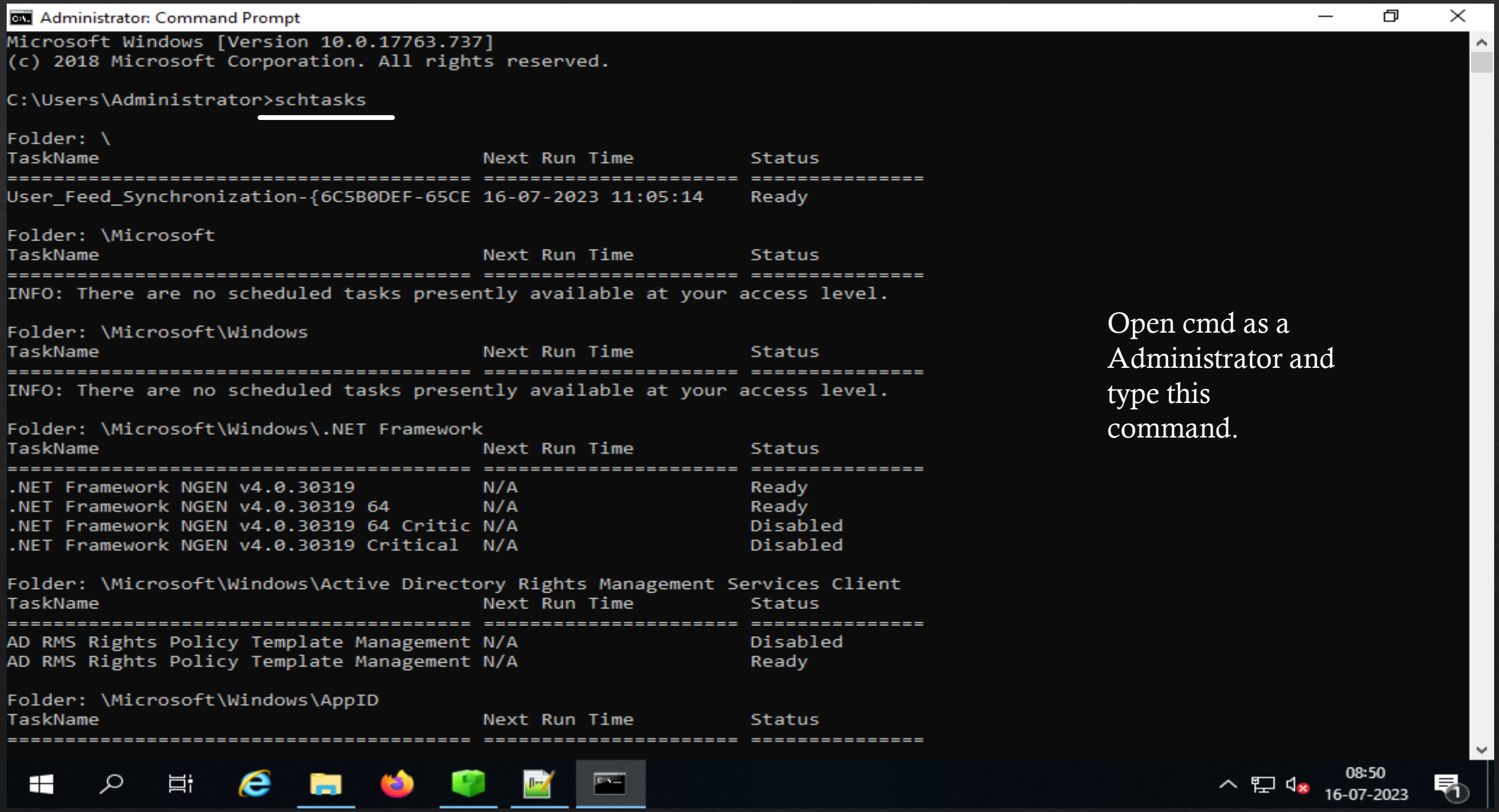

Registry Explorer v1.6.0.0
File Tools Options Bookmarks (29/0) View Help
Registry hives (1) Available bookmarks (29/0)
Find
Key name
SafeBoot
Services
.NET CLR Data
.NET CLR Networking
.NET CLR Networking 4.0.0.0
.NET Data Provider for Oracle
.NET Data Provider for SqlServer
.NET Memory Cache 4.0
.NETFramework
1394ohci
Bookmark information
Hive C:\Cases\Analysis\Registry\SYSTEM
Category Operating system
Name Services
Key path ControlSet001\Services
Short description Service definitions and parameters
Long description
Values Services
Drag a column header here to group by that column
Name Descri... Display... Start ... Servic... Name ... Param... Group Image ... Servic... Require...
3ware Boot Kernel... 2023-0... 2019-1... SCSI miniport System32\drivers\3ware.sys
AarSvc @%SystemRoot%\system32\AarSvc.dll,-101 @%SystemRoot%\system32\AarSvc.dll,-100 Manual 96 2019-1... 2019-1... %SystemRoot%\system32\svchost.exe -k AarSvcGroup -p %SystemRoot%\System32\AarSvc.dll SeImpersonatePrivilege
ACPI @acpi.inf,%ACPI.SvcDesc%;Microsoft ACPI Driver Boot Kernel... 2023-0... 2023-0... Core System32\drivers\ACPI.sys
AcpiDev @acpidev.inf,%AcpiDev. Manual Kernel... 2019-1... Extended Base \SystemRoot\System32\
Total rows: 691
Export ?
Type viewer
Loaded the system hives in Registry Explorer
07:54
16-07-2023



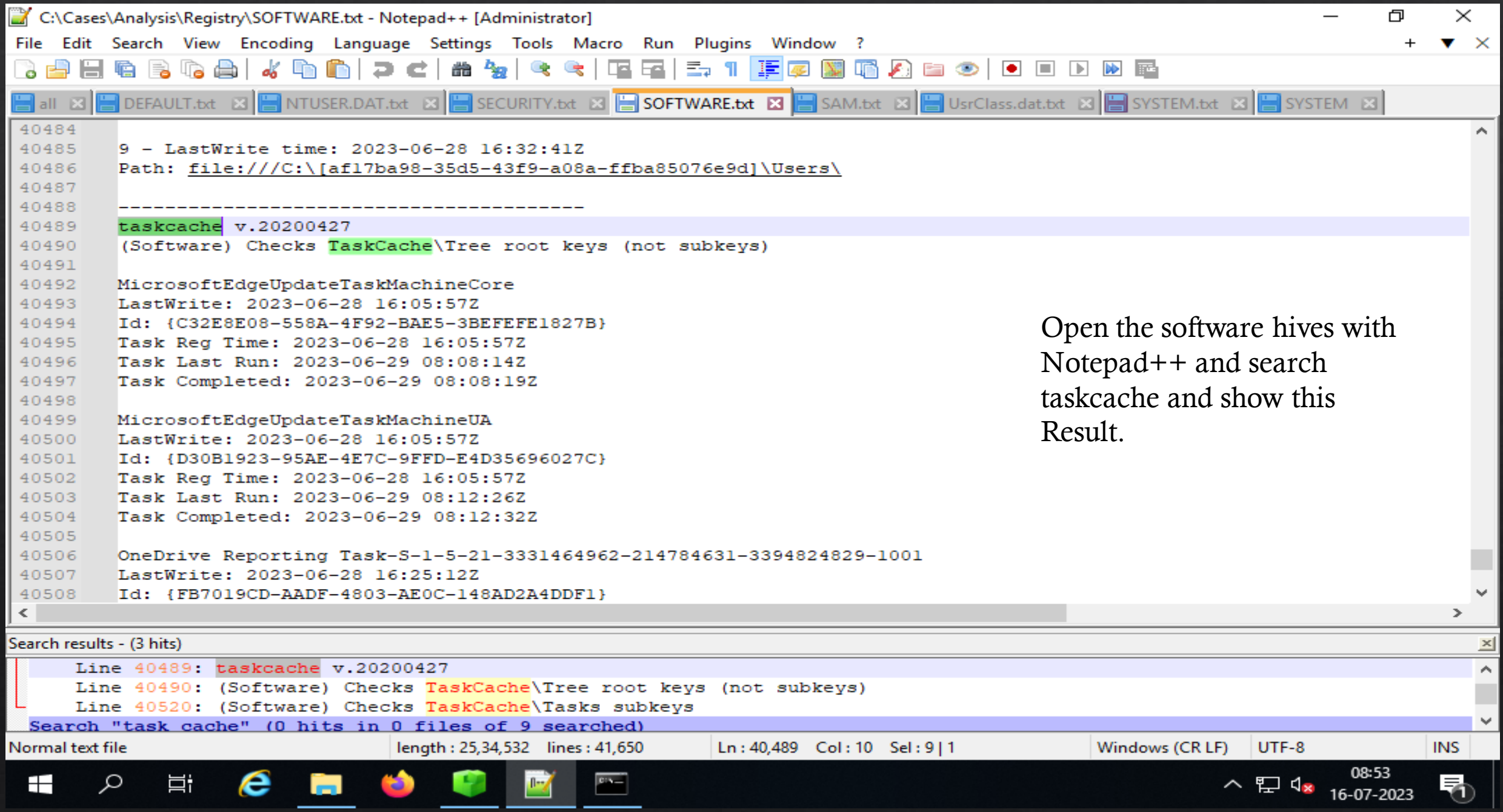
System hives edit with Notepad++ and Find the services on target system and show the given output.

Detecting and Analyzing scheduled tasks





Open cmd as a Administrator and type this command.



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 - | english to gujarati translate - Go | Autoruns for Windows - Sysinter

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

Download PDF

Usage
Autorunsc Usage
Related Links
Download

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

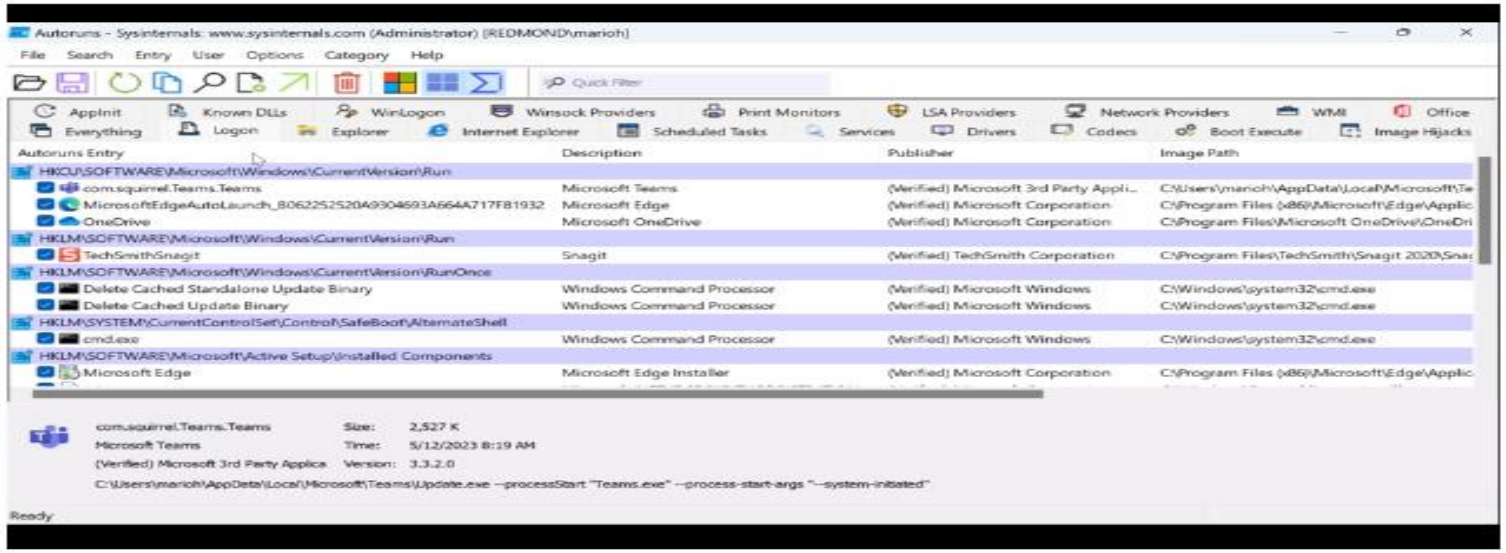
By Mark Russinovich

Published: June 27, 2023

Download Autoruns and Autorunsc (2.8 MB)

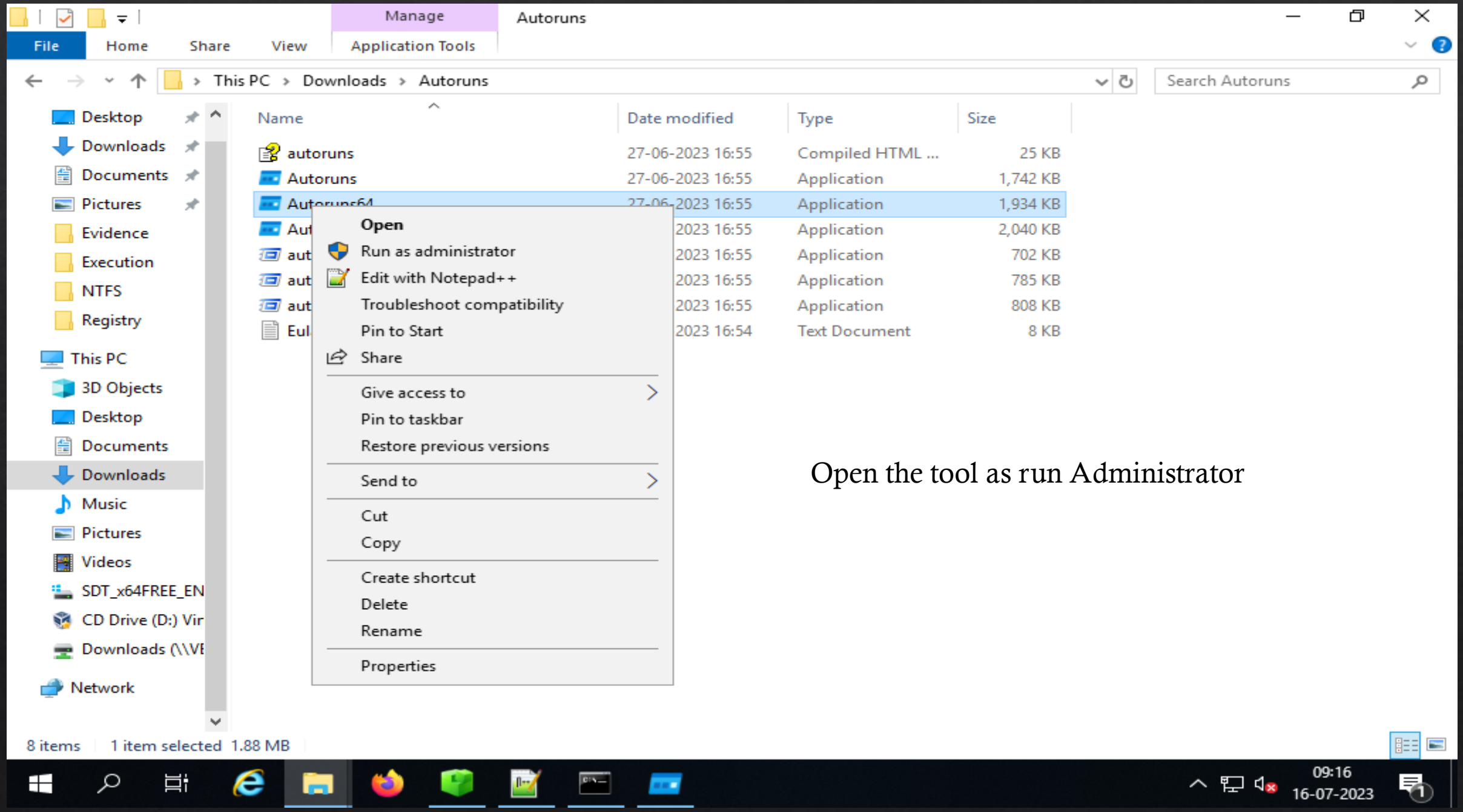
Run now from Sysinternals Live.

Download the tool from microsoft

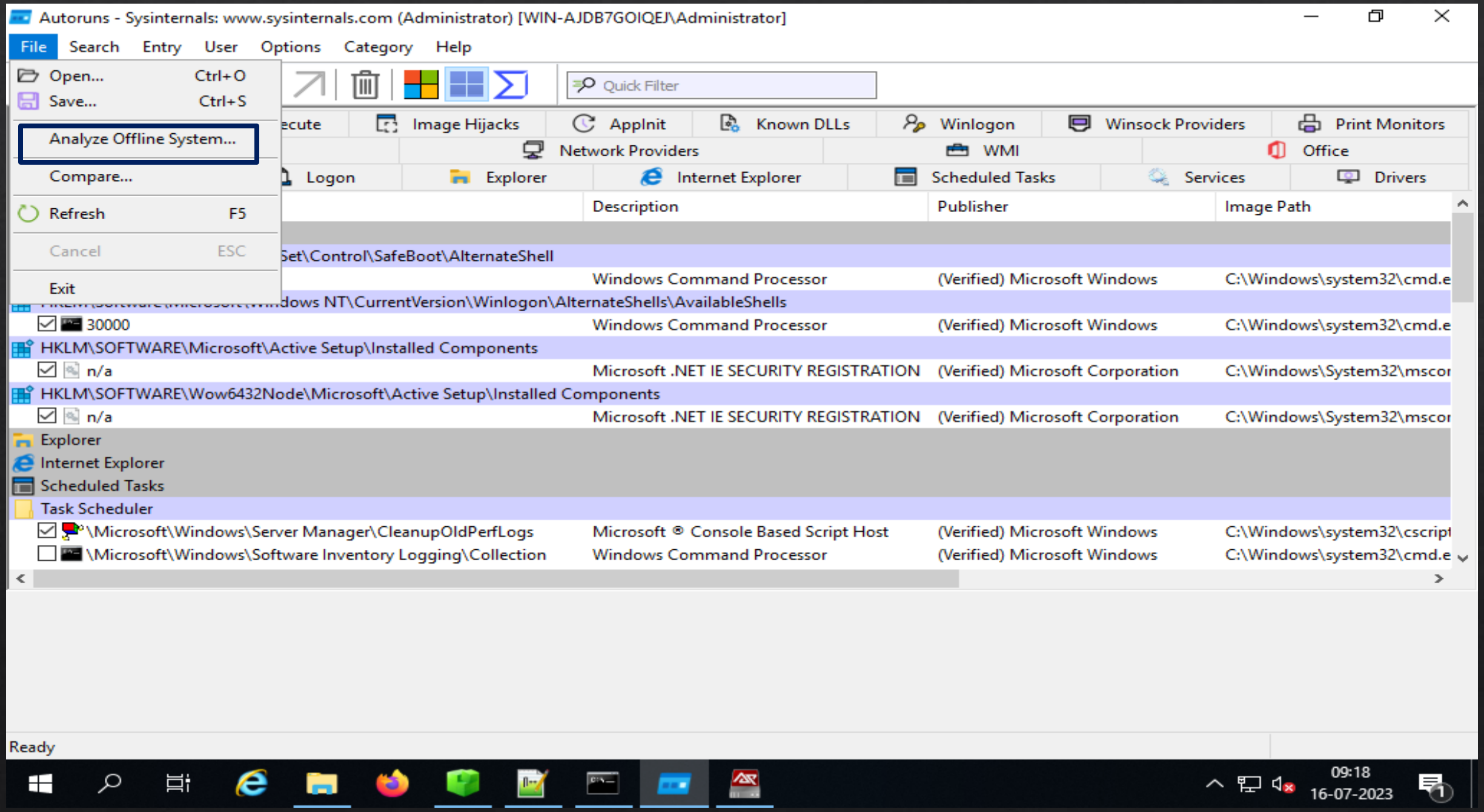


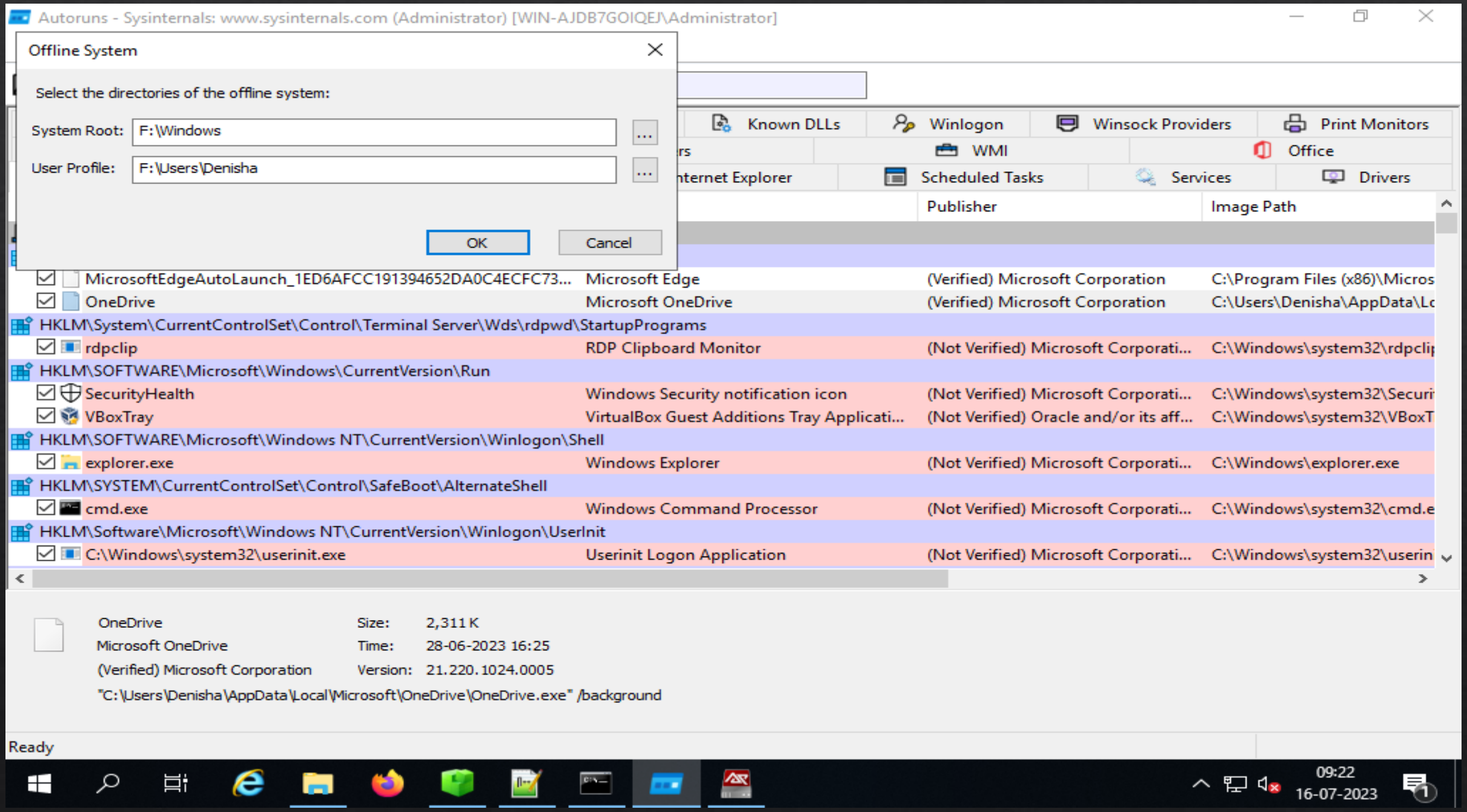
Type here to search

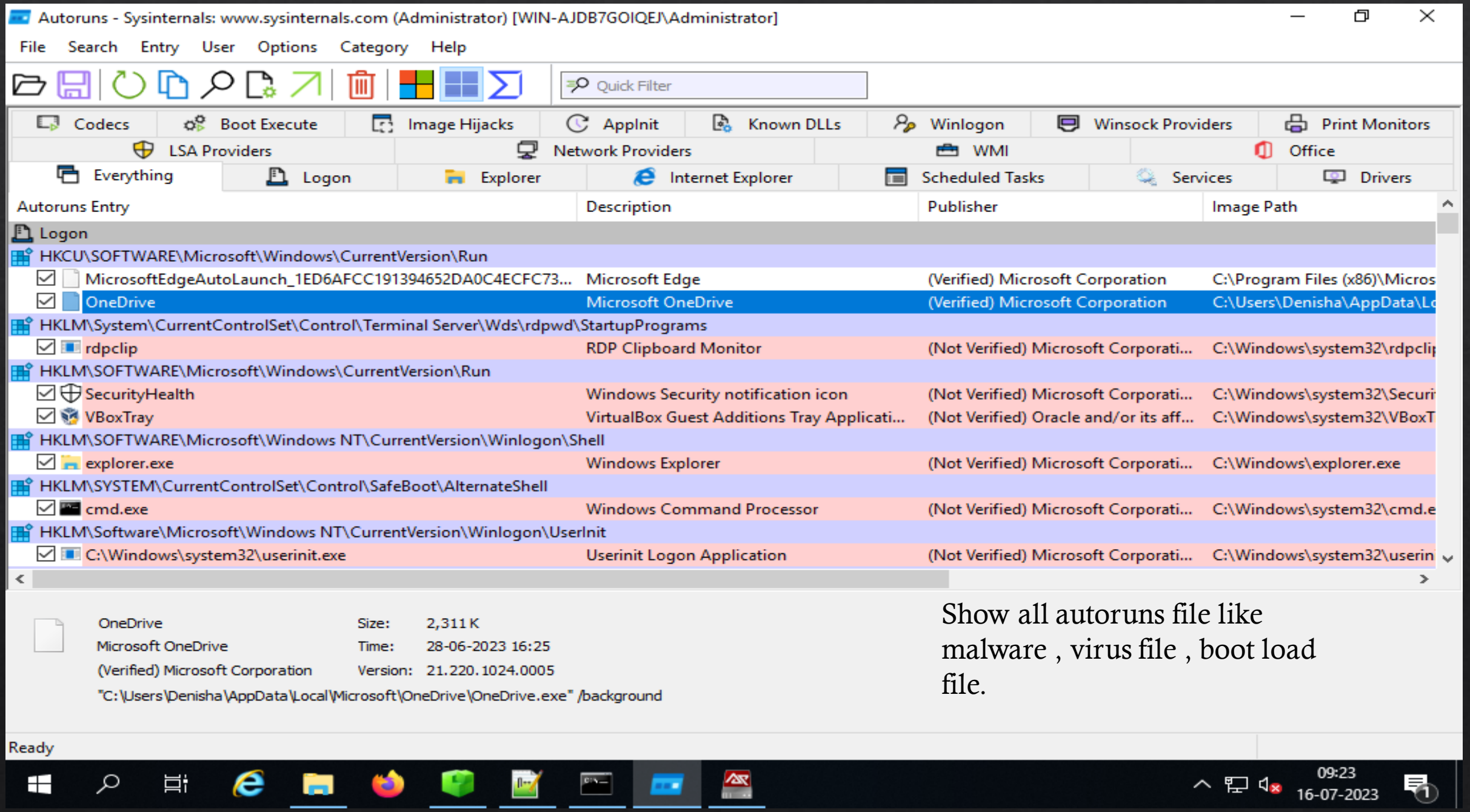
14:44
16-07-2023



Open the tool as run Administrator


Autoruns - Sysinternals: www.sysinternals.com (Administrator) [WIN-AJDB7GOIQEJ\Administrator]
File
Search
Entry
User
Options
Category
Help
Open... Ctrl+O
Save... Ctrl+S
Analyze Offline System...
Compare...
Refresh F5
Cancel ESC
Exit
Quick Filter
Image Hijacks
AppInit
Known DLLs
Winlogon
Winsock Providers
Print Monitors
Network Providers
WMI
Office
Logon
Explorer
Internet Explorer
Scheduled Tasks
Services
Drivers
Description
Publisher
Image Path
Windows Command Processor
(Verified) Microsoft Windows
C:\Windows\system32\cmd.e
30000
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
n/a
Microsoft .NET IE SECURITY REGISTRATION
(Verified) Microsoft Corporation
C:\Windows\System32\mscor
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components
Explorer
Internet Explorer
Scheduled Tasks
Task Scheduler
\Microsoft\Windows\Server Manager\CleanupOldPerfLogs
Microsoft ® Console Based Script Host
C:\Windows\system32\cscript
\Microsoft\Windows\Software Inventory Logging\Collection
Ready
09:18
16-07-2023


Autoruns - Sysinternals: www.sysinternals.com (Administrator) [WIN-AJDB7GOIQEJ\Administrator]
Offline System
Select the directories of the offline system:
System Root: F:\Windows
User Profile: F:\Users\Denisha
OK
Cancel
Known DLLs
Winlogon
Winsock Providers
Print Monitors
WMI
Office
Scheduled Tasks
Services
Drivers
Publisher
Image Path
MicrosoftEdgeAutoLaunch_1ED6AFCC191394652DA0C4ECFC73... Microsoft Edge (Verified) Microsoft Corporation C:\Program Files (x86)\Micros
OneDrive Microsoft OneDrive (Verified) Microsoft Corporation C:\Users\Denisha\AppData\Lo
HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms
rdpclip RDP Clipboard Monitor (Not Verified) Microsoft Corporati... C:\Windows\system32\rdpclip
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SecurityHealth Windows Security notification icon (Not Verified) Microsoft Corporati... C:\Windows\system32\Securi
VBoxTray VirtualBox Guest Additions Tray Applicati... (Not Verified) Oracle and/or its aff... C:\Windows\system32\VBoxT
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
explorer.exe Windows Explorer (Not Verified) Microsoft Corporati... C:\Windows\explorer.exe
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell
cmd.exe Windows Command Processor (Not Verified) Microsoft Corporati... C:\Windows\system32\cmd.e
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userlnit
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

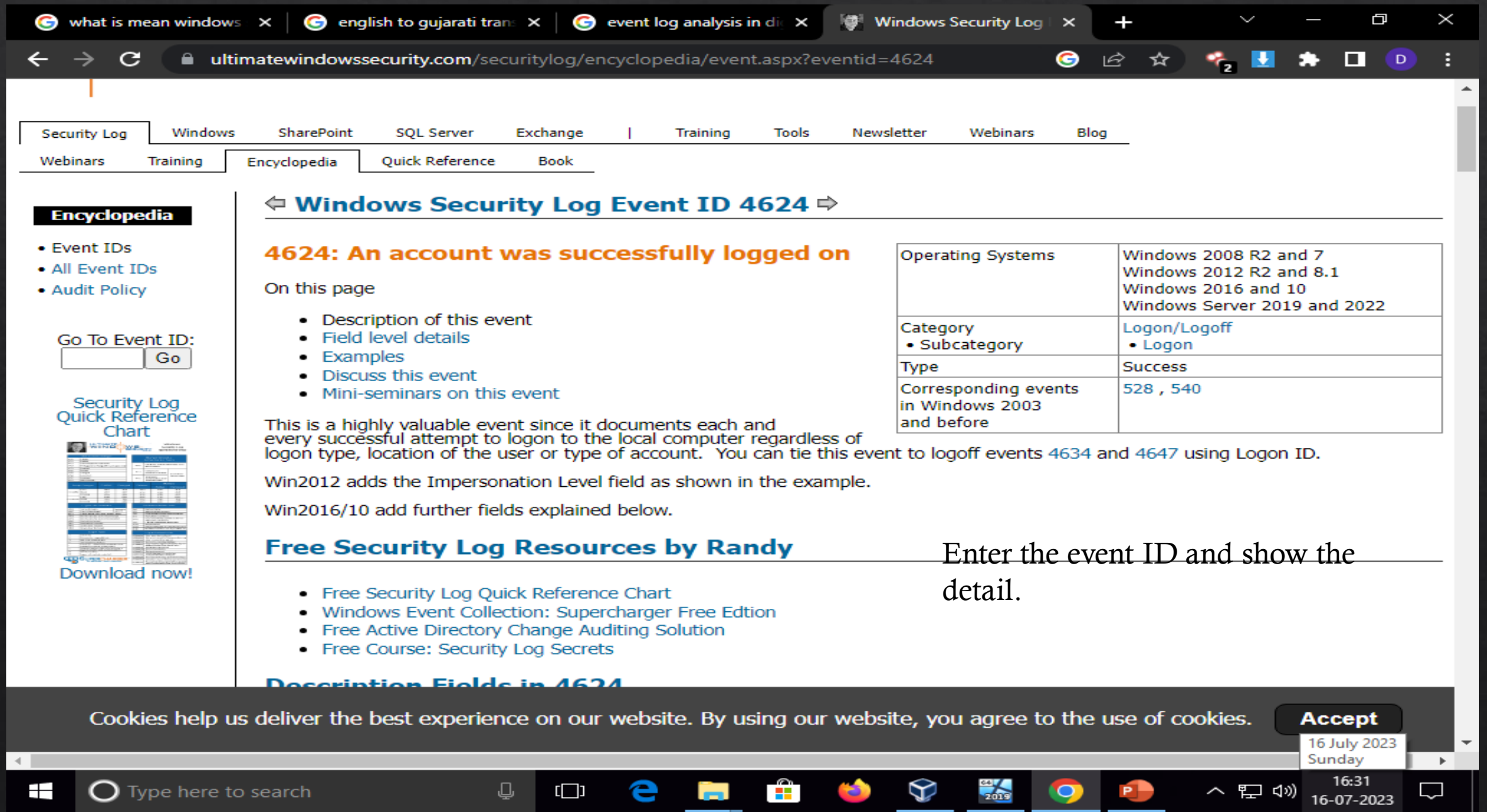


Show all autoruns file like malware , virus file , boot load file.

Event log Analysis

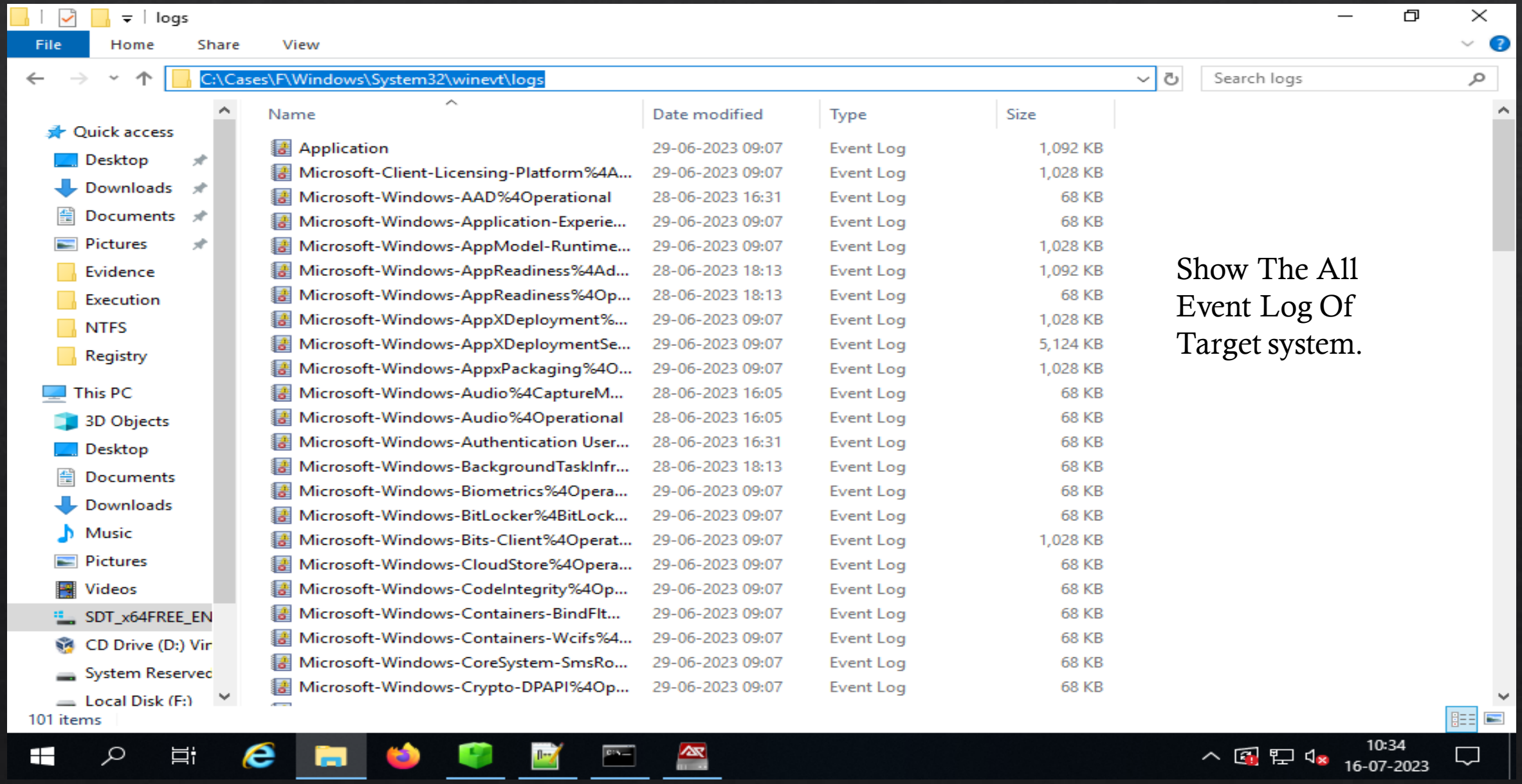
The main purpose of the event logs is to provide information to administrators and users. They are structured in five levels (information, warning, error, critical, and success/failure audit). In terms of forensic analysis, this is a valuable source to understand the course of actions on a system.

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

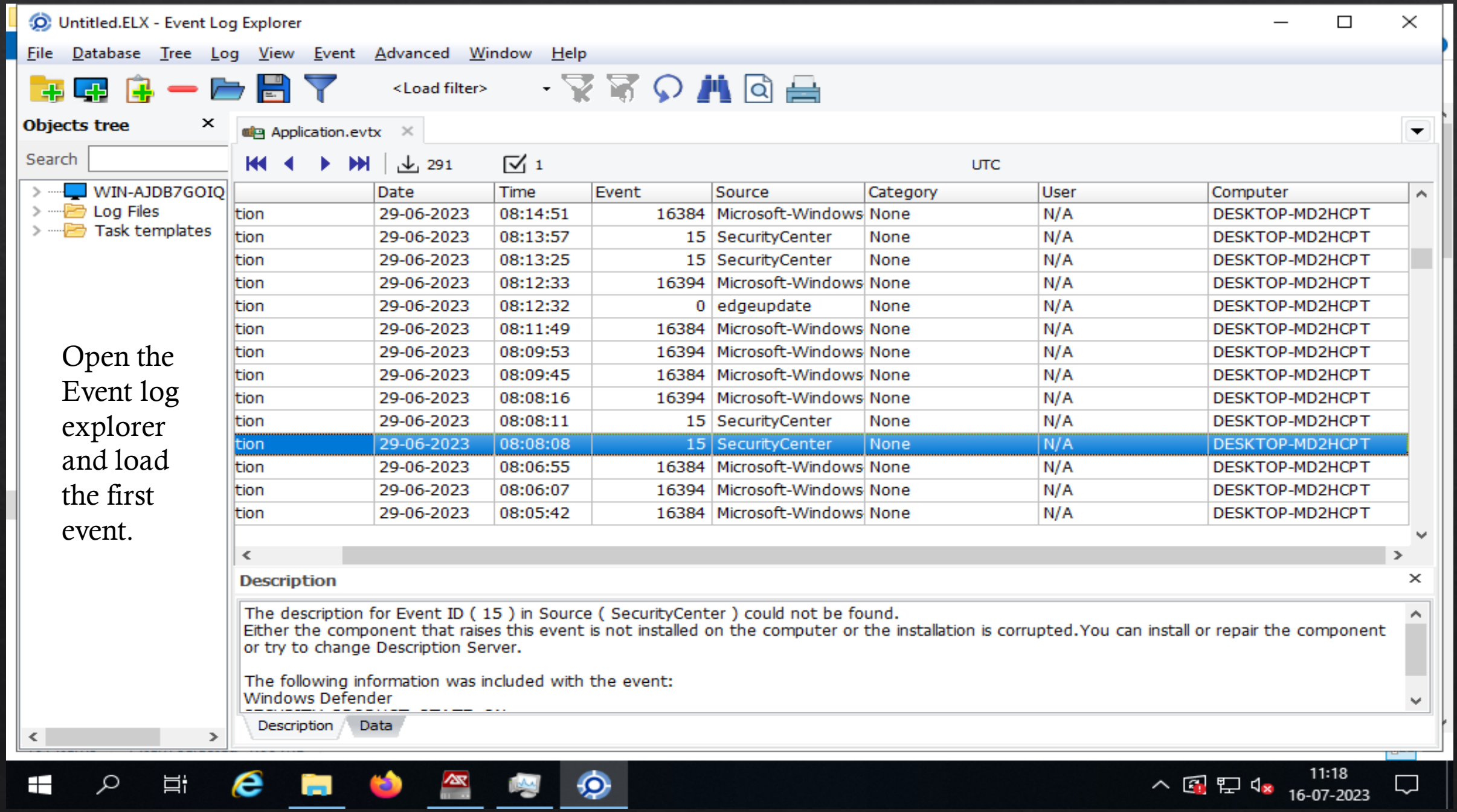


Enter the event ID and show the detail.

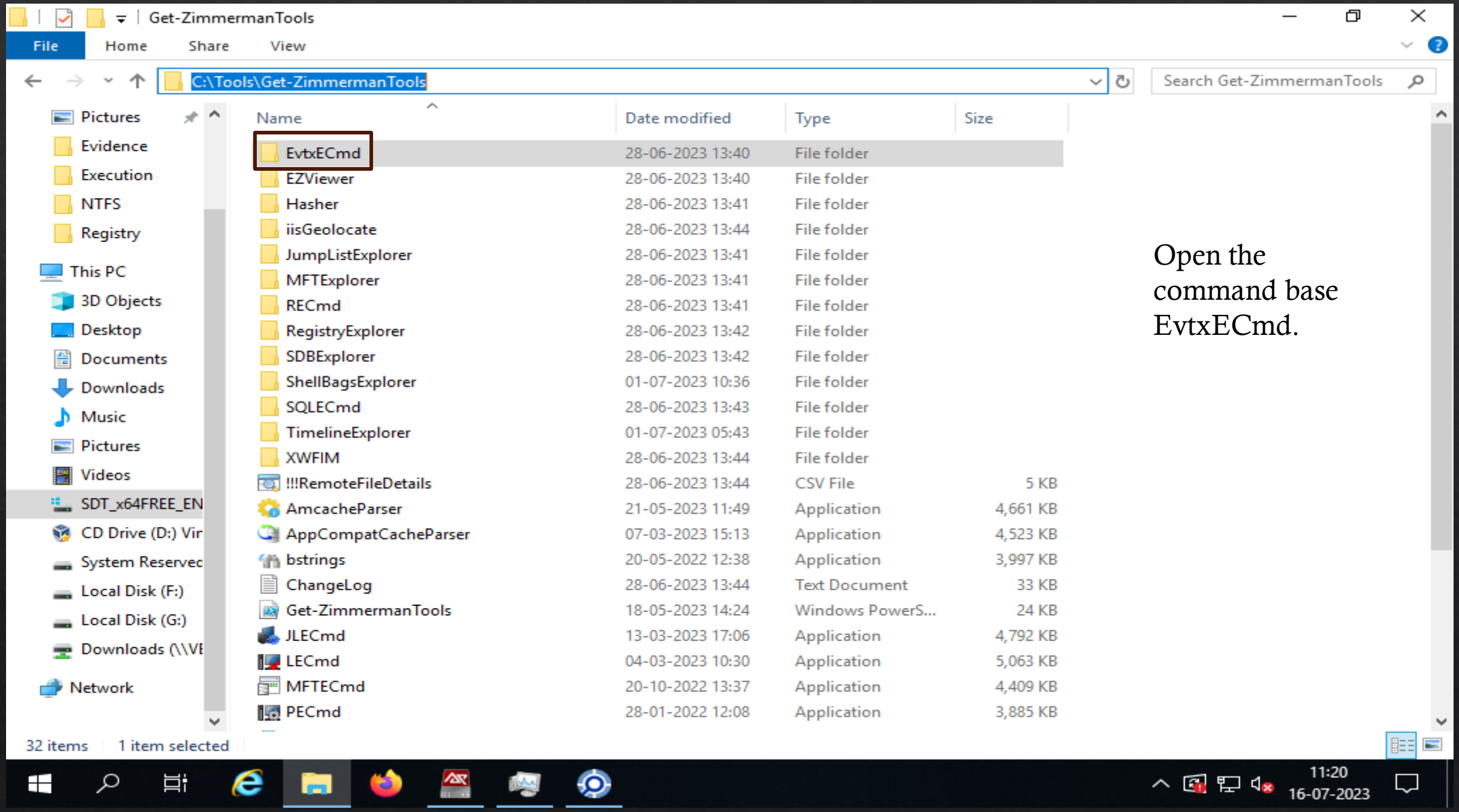
Analyzing Windows event logs with EventLogExplorer and EvtxCmd



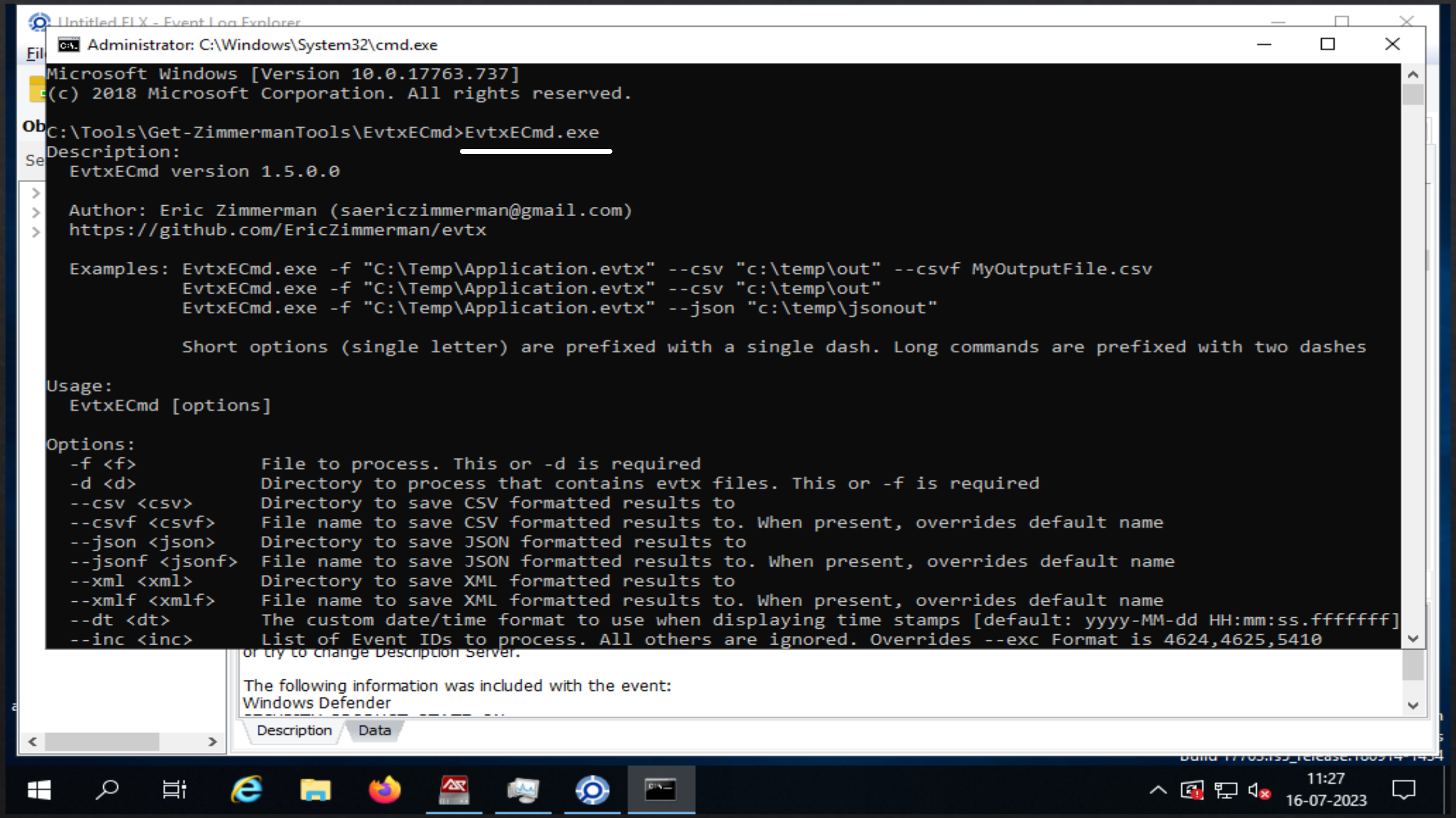
Show The All Event Log Of Target system.

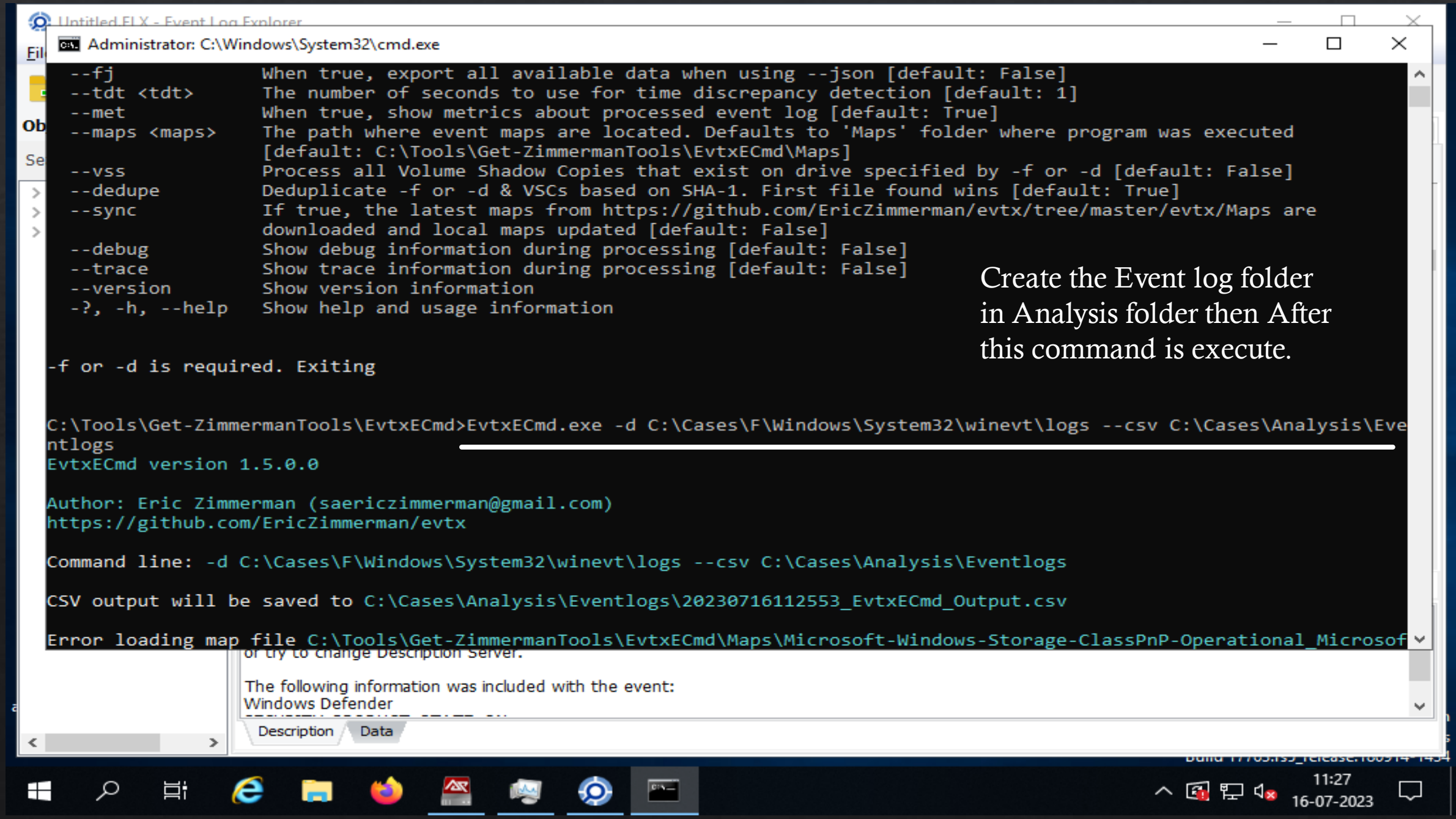


Open the Event log explorer and load the first event.

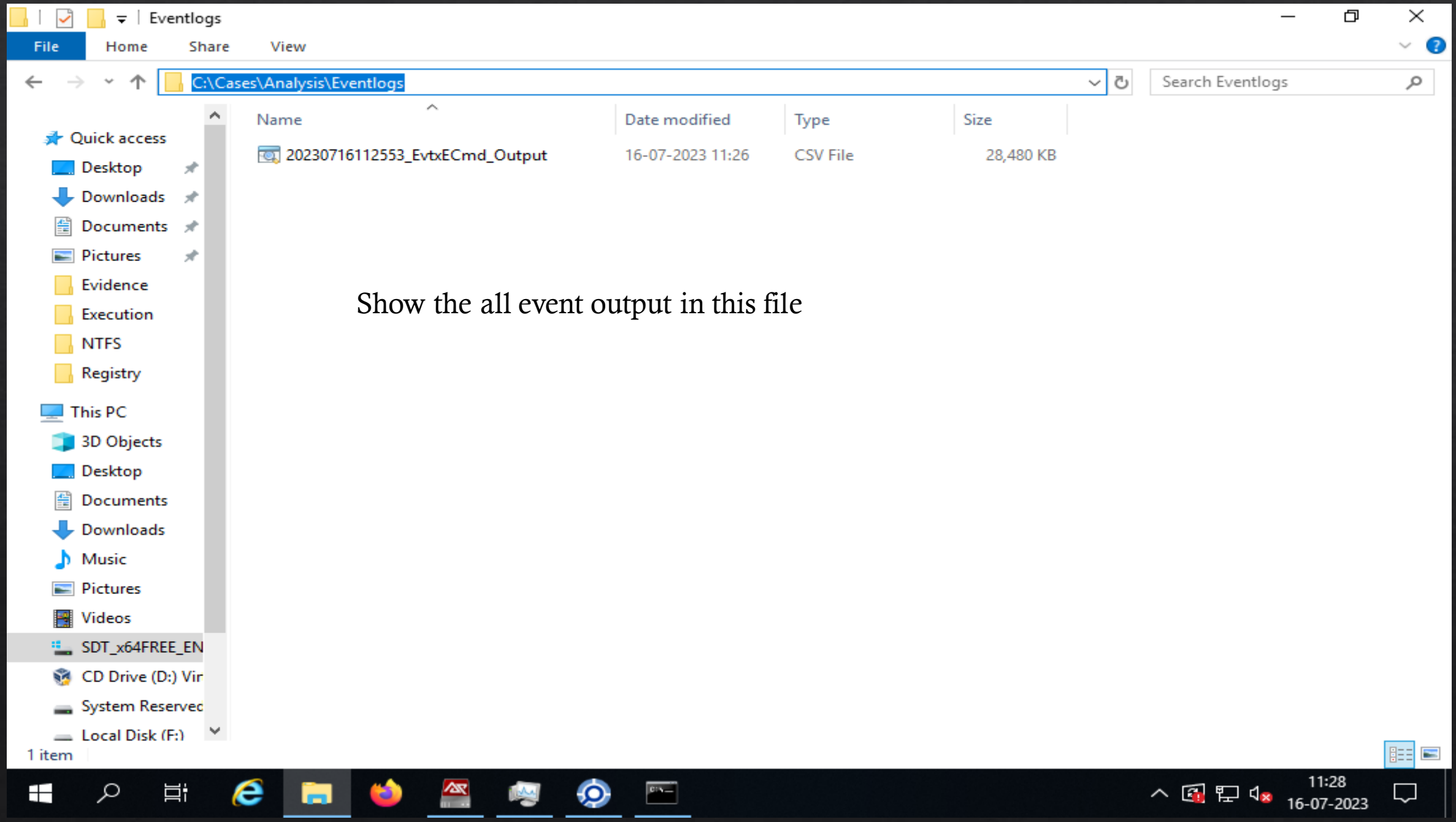


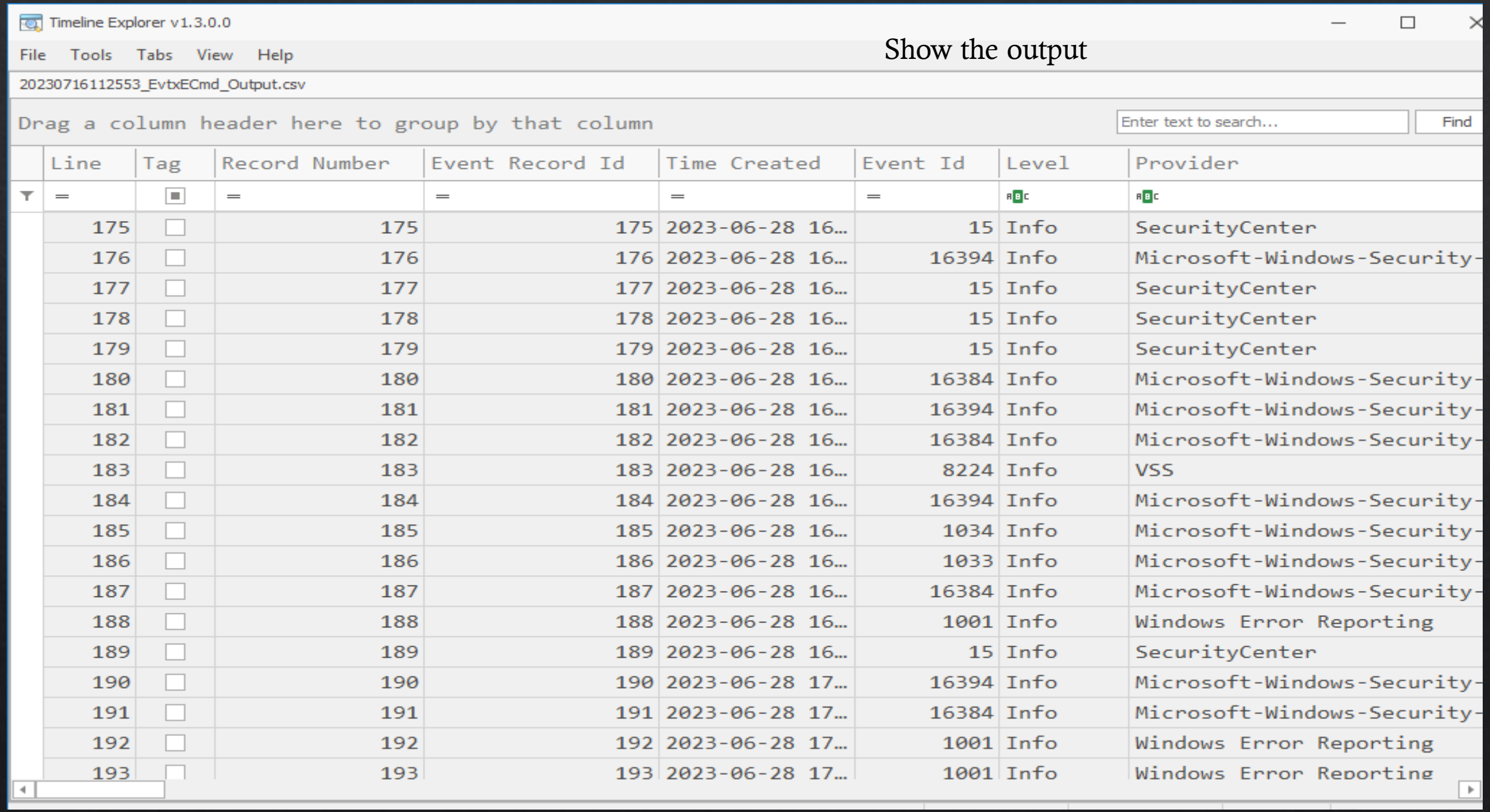
Open the command base EvtxECmd.


Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Tools\Get-ZimmermanTools\EvtxECmd>EvtxECmd.exe
Description:
EvtxECmd version 1.5.0.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/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.fffffff]
--inc <inc> List of Event IDs to process. All others are ignored. Overrides --exc Format is 4624,4625,5410
The following information was included with the event:
Windows Defender
Description
Data
11:27
16-07-2023



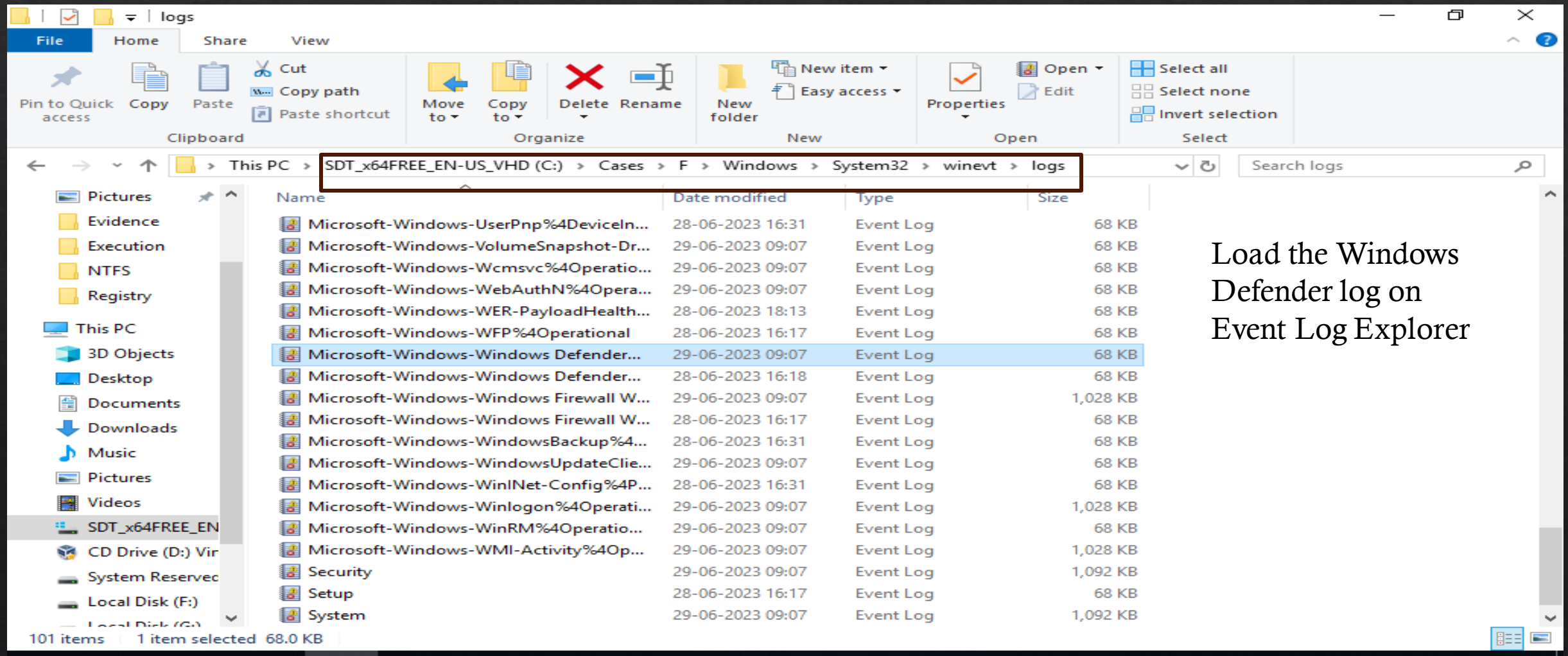
Create the Event log folder in Analysis folder then After this command is execute.


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 Reservec
Local Disk (F:)
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
1 item
11:28
16-07-2023


Timeline Explorer v1.3.0.0
File Tools Tabs View Help
Show the output
20230716112553_EvtxECmd_Output.csv
Drag a column header here to group by that column
Enter text to search...
Find
Line | Tag | Record Number | Event Record Id | Time Created | Event Id | Level | Provider
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

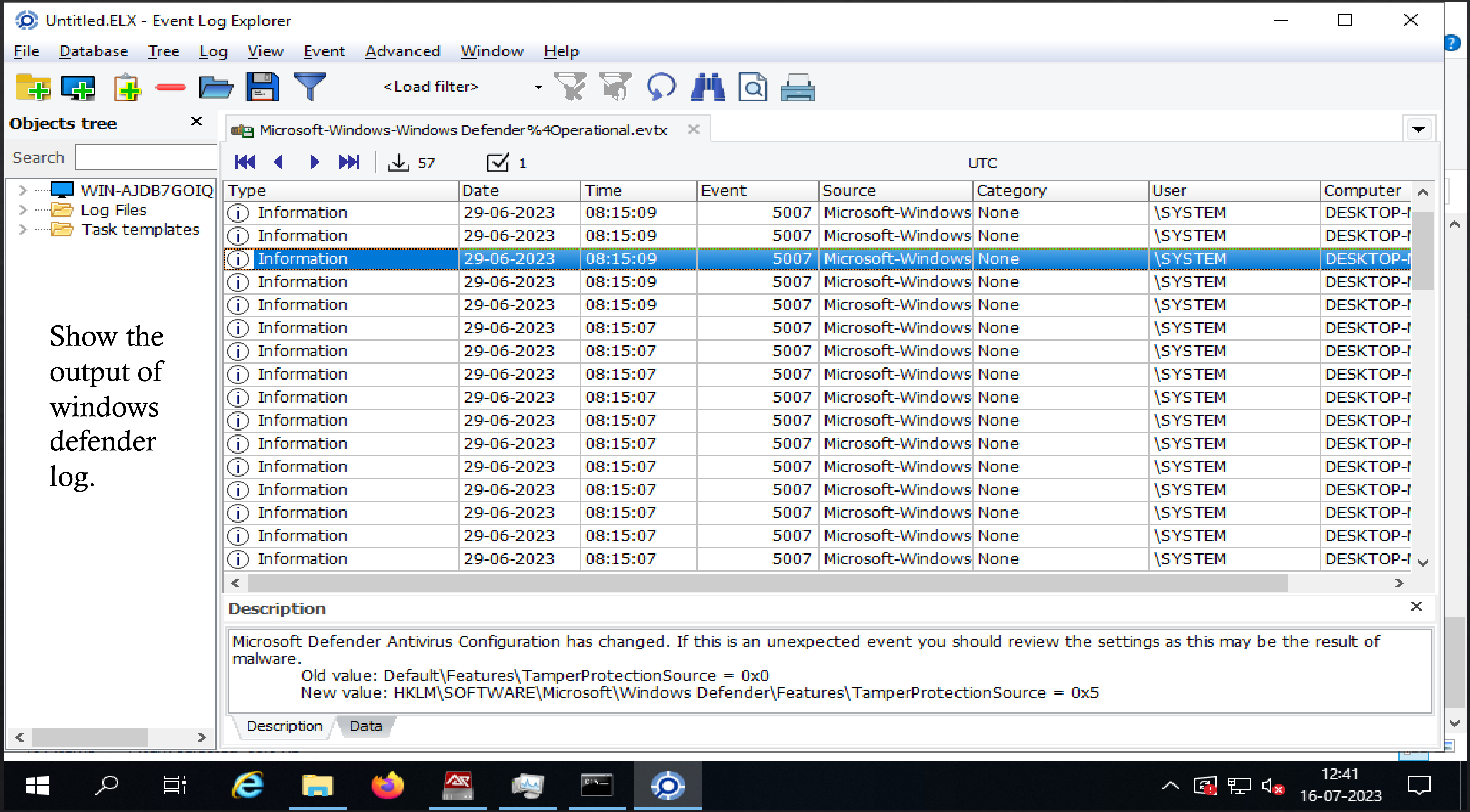
1. Windows Event Logs Defender Analysis

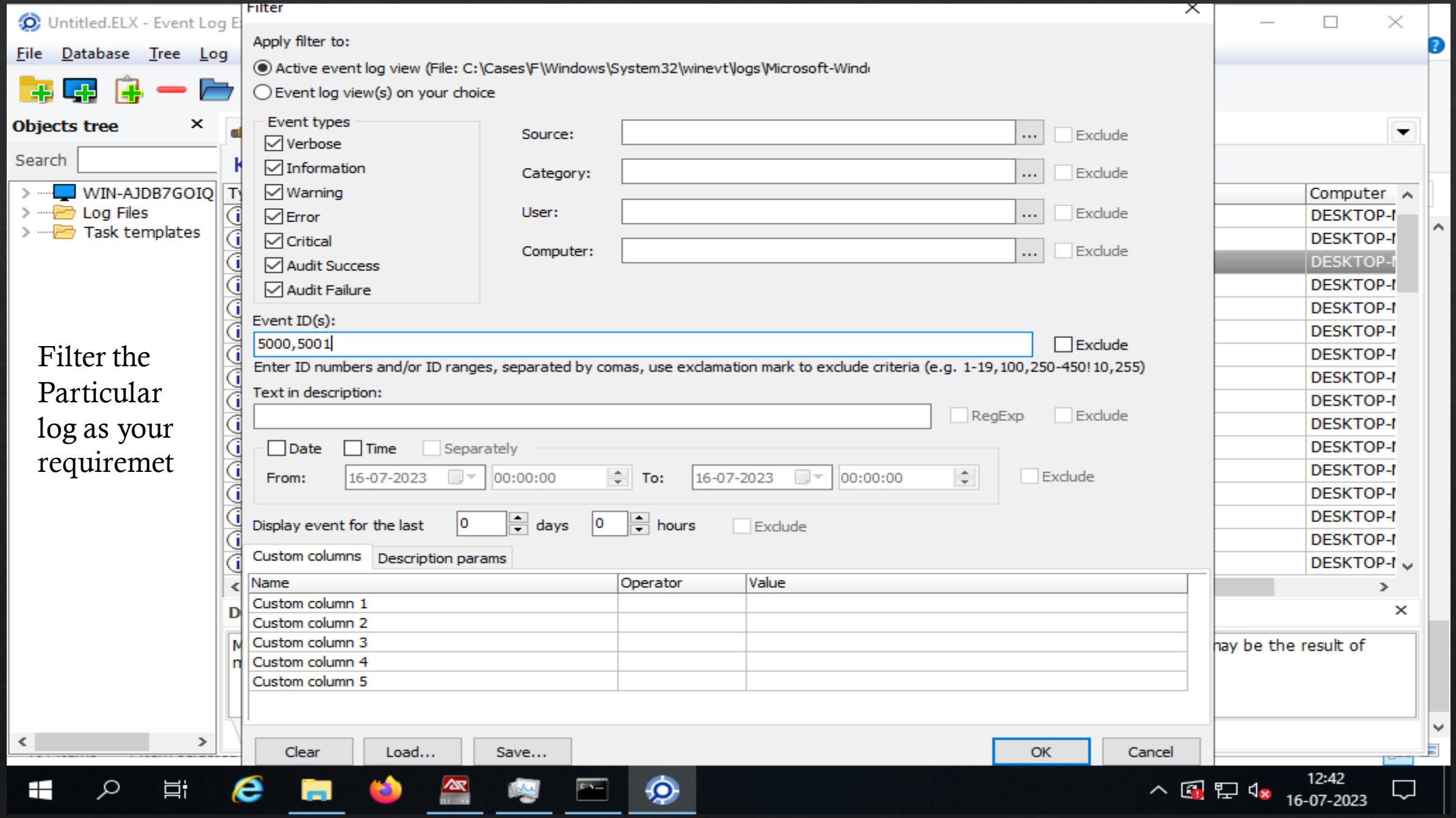
Source	Event IDs	Description
Microsoft-Windows-Windows Defender	5000	Defender enabled
	5001	Defender disabled



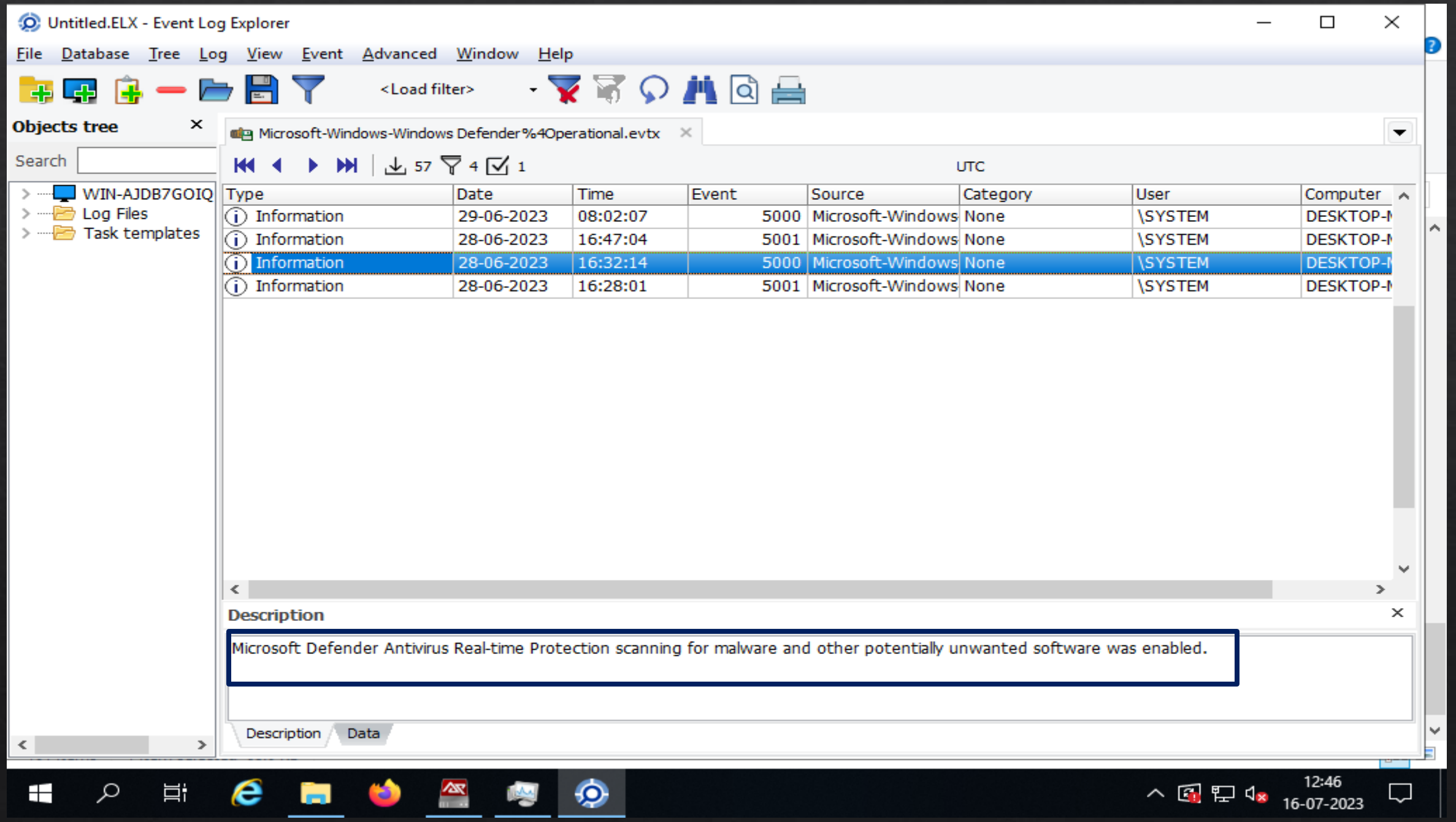
Load the Windows Defender log on Event Log Explorer

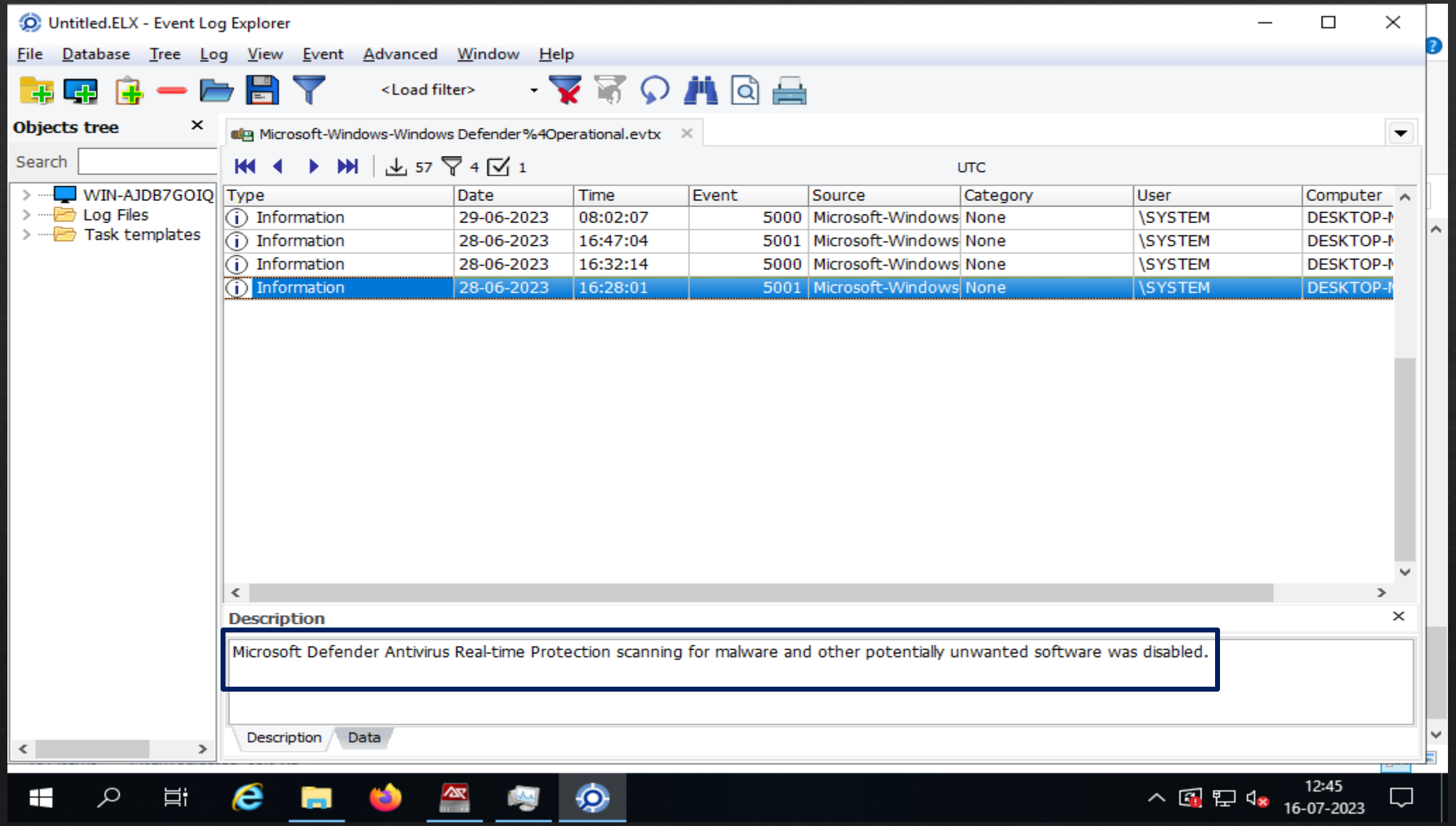
Show the output of windows defender log.





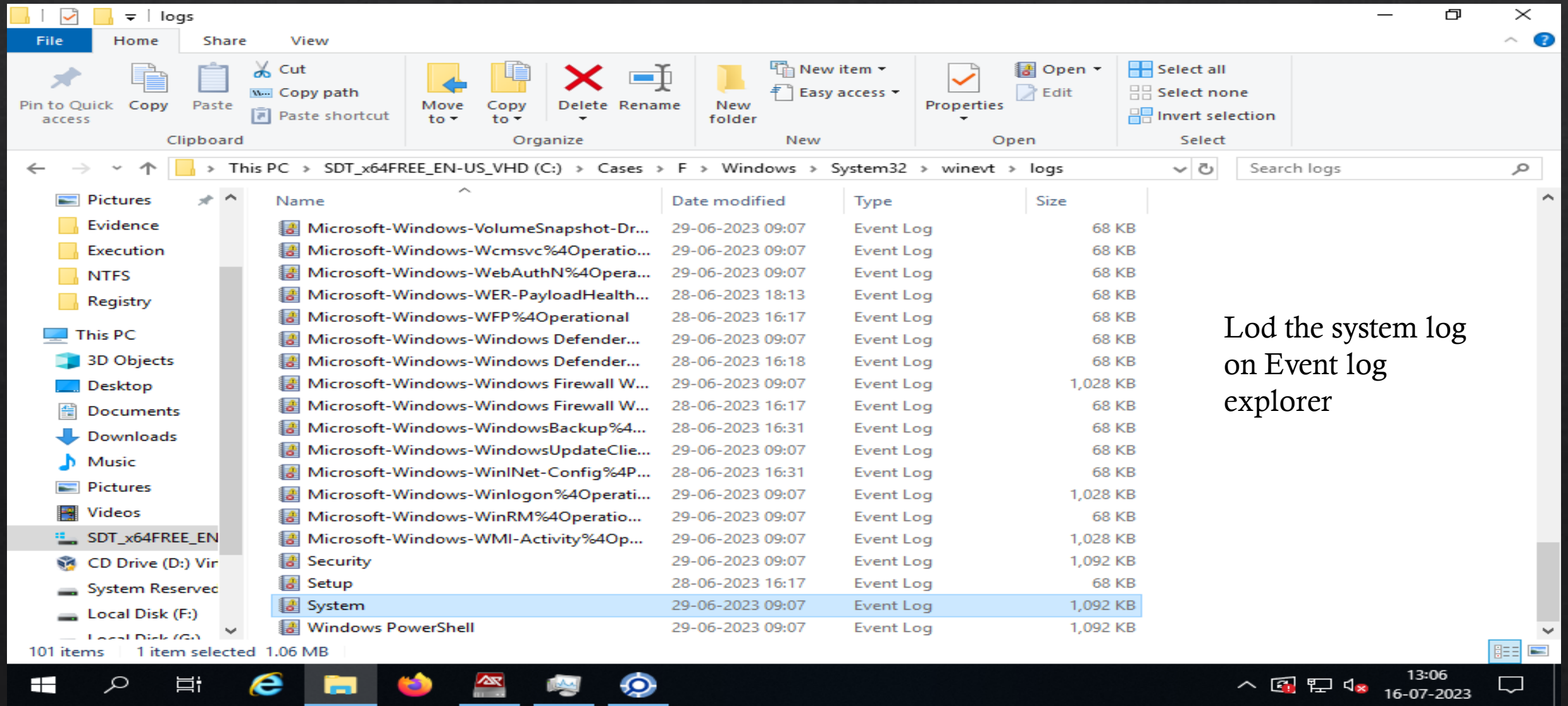
Filter the Particular log as your requiremet


Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
<Load filter>
Objects tree
Search
WIN-AJDB7GOIQ
Log Files
Task templates
Microsoft-Windows-Windows Defender%4Operational.evtx
57 4 1
UTC
Type Date Time Event Source Category User Computer
Information 29-06-2023 08:02:07 5000 Microsoft-Windows None \SYSTEM DESKTOP-
Information 28-06-2023 16:47:04 5001 Microsoft-Windows None \SYSTEM DESKTOP-
Information 28-06-2023 16:32:14 5000 Microsoft-Windows None \SYSTEM DESKTOP-
Information 28-06-2023 16:28:01 5001 Microsoft-Windows None \SYSTEM DESKTOP-
Description
Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was enabled.
Description Data
12:46
16-07-2023

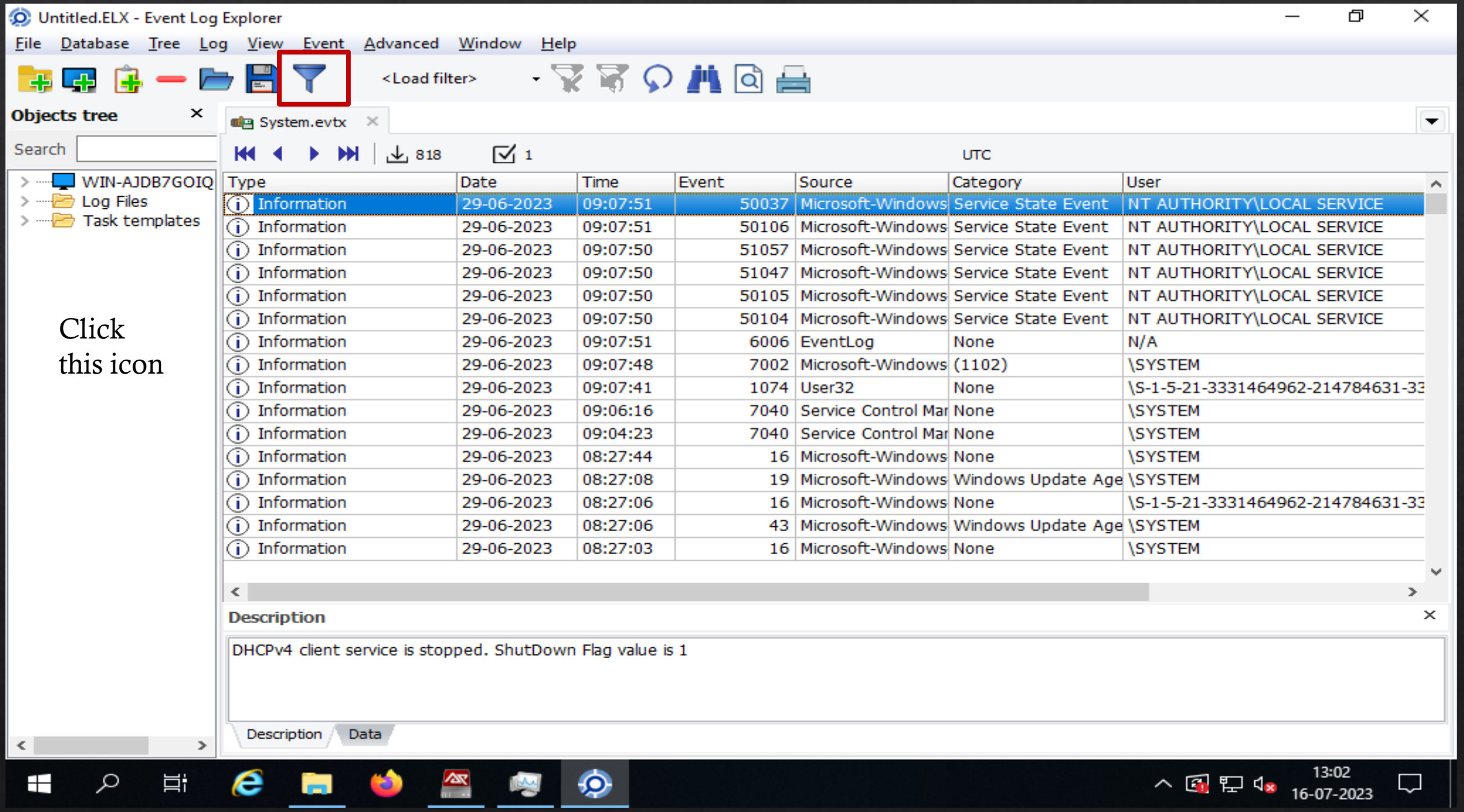

Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
<Load filter>
Objects tree
Search
WIN-AJDB7GOIQ
Log Files
Task templates
Microsoft-Windows-Windows Defender%4Operational.evtx
57 4 1
UTC
Type Date Time Event Source Category User Computer
Information 29-06-2023 08:02:07 5000 Microsoft-Windows None \SYSTEM DESKTOP-
Information 28-06-2023 16:47:04 5001 Microsoft-Windows None \SYSTEM DESKTOP-
Information 28-06-2023 16:32:14 5000 Microsoft-Windows None \SYSTEM DESKTOP-
Information 28-06-2023 16:28:01 5001 Microsoft-Windows None \SYSTEM DESKTOP-
Description
Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.
Description Data
12:45
16-07-2023

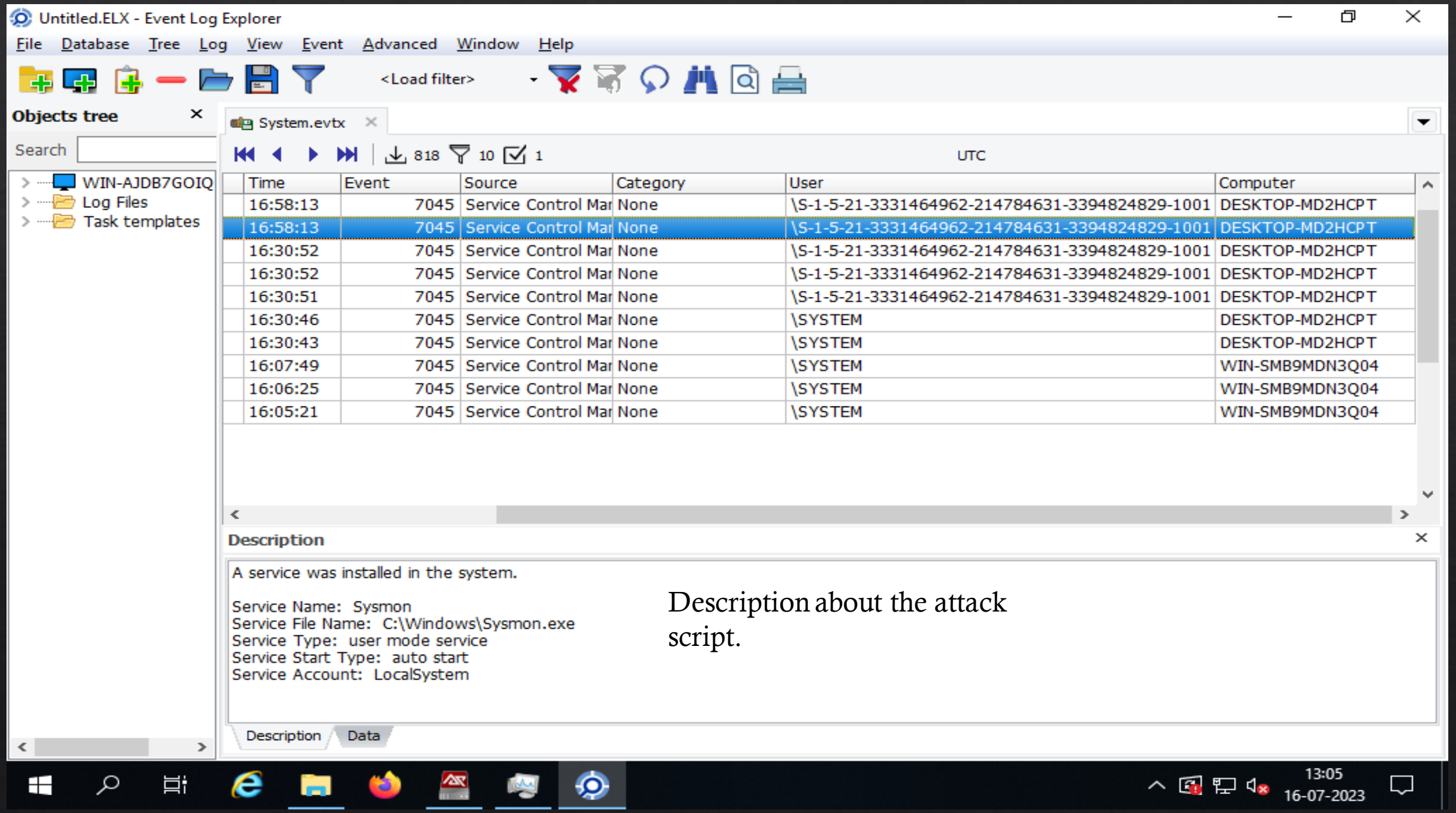
2. System log Analysis

Source	Event IDs	Description
System	7045	A new service was installed



Lod the system log on Event log explorer

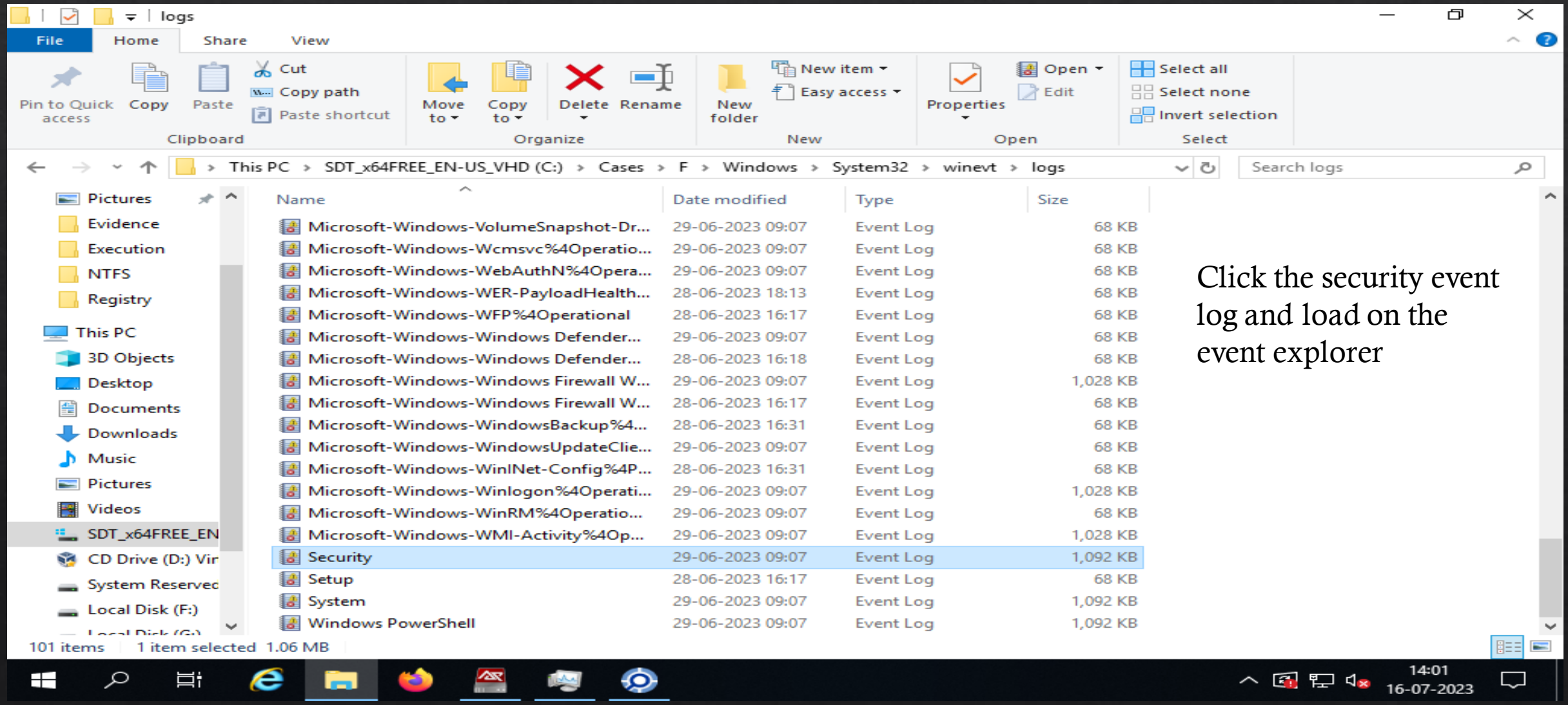

Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
<Load filter>
Objects tree
Search
WIN-AJDB7GOIQ
Log Files
Task templates
Click this icon
System.evtx
818
1
UTC
Type Date Time Event Source Category User
Information 29-06-2023 09:07:51 50037 Microsoft-Windows Service State Event NT AUTHORITY\LOCAL SERVICE
Information 29-06-2023 09:07:51 50106 Microsoft-Windows Service State Event NT AUTHORITY\LOCAL SERVICE
Information 29-06-2023 09:07:50 51057 Microsoft-Windows Service State Event NT AUTHORITY\LOCAL SERVICE
Information 29-06-2023 09:07:50 51047 Microsoft-Windows Service State Event NT AUTHORITY\LOCAL SERVICE
Information 29-06-2023 09:07:50 50105 Microsoft-Windows Service State Event NT AUTHORITY\LOCAL SERVICE
Information 29-06-2023 09:07:50 50104 Microsoft-Windows Service State Event NT AUTHORITY\LOCAL SERVICE
Information 29-06-2023 09:07:51 6006 EventLog None N/A
Information 29-06-2023 09:07:48 7002 Microsoft-Windows (1102) \SYSTEM
Information 29-06-2023 09:07:41 1074 User32 None \S-1-5-21-3331464962-214784631-33
Information 29-06-2023 09:06:16 7040 Service Control Mar None \SYSTEM
Information 29-06-2023 09:04:23 7040 Service Control Mar None \SYSTEM
Information 29-06-2023 08:27:44 16 Microsoft-Windows None \SYSTEM
Information 29-06-2023 08:27:08 19 Microsoft-Windows Windows Update Age \SYSTEM
Information 29-06-2023 08:27:06 16 Microsoft-Windows None \S-1-5-21-3331464962-214784631-33
Information 29-06-2023 08:27:06 43 Microsoft-Windows Windows Update Age \SYSTEM
Information 29-06-2023 08:27:03 16 Microsoft-Windows None \SYSTEM
Description
DHCPv4 client service is stopped. ShutDown Flag value is 1
Description Data
13:02
16-07-2023



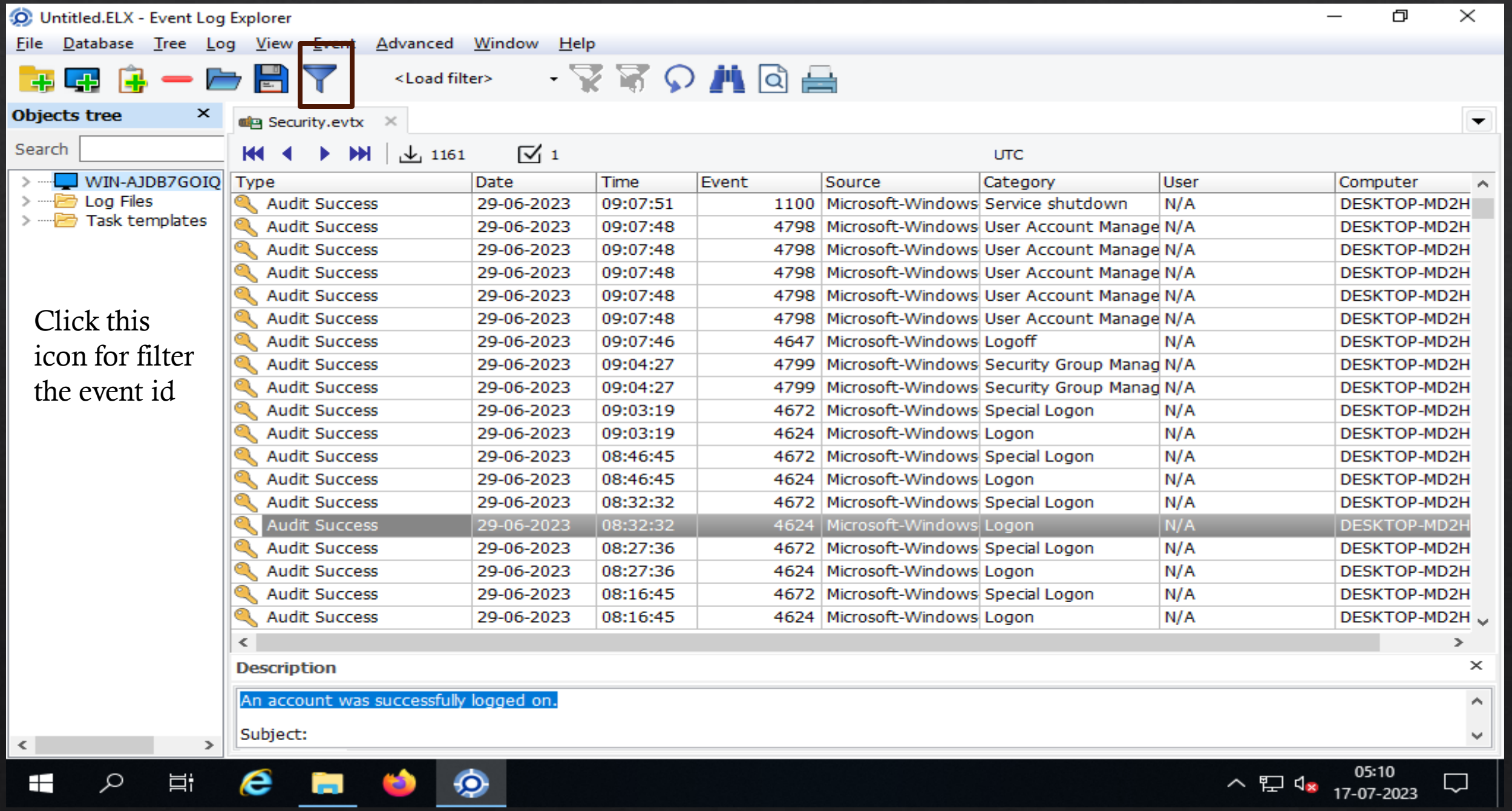
Description about the attack script.

3. Security and Authentication Event logs

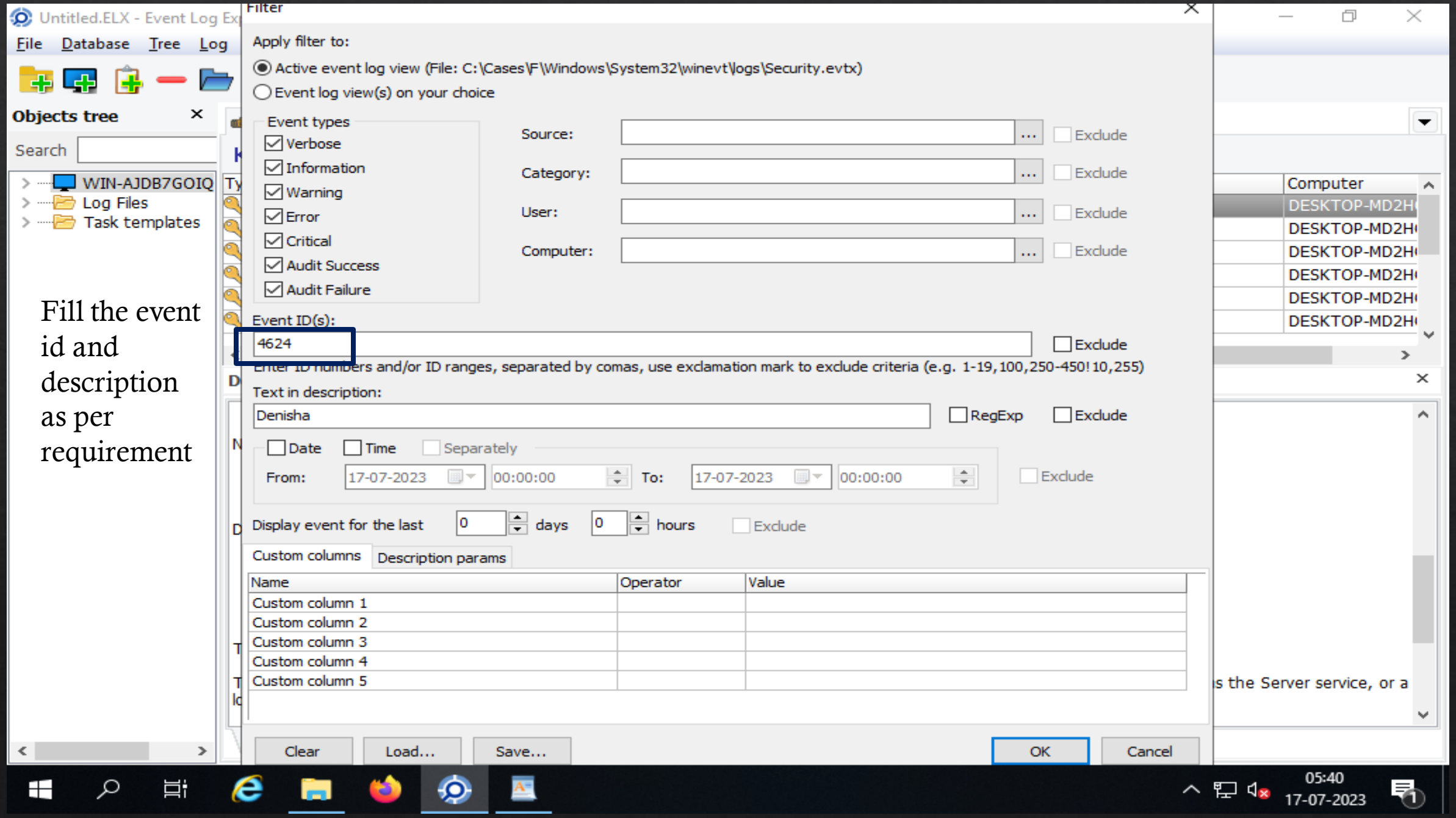
Source	Event IDs	Description
Security	4624	An account was successfully logged on



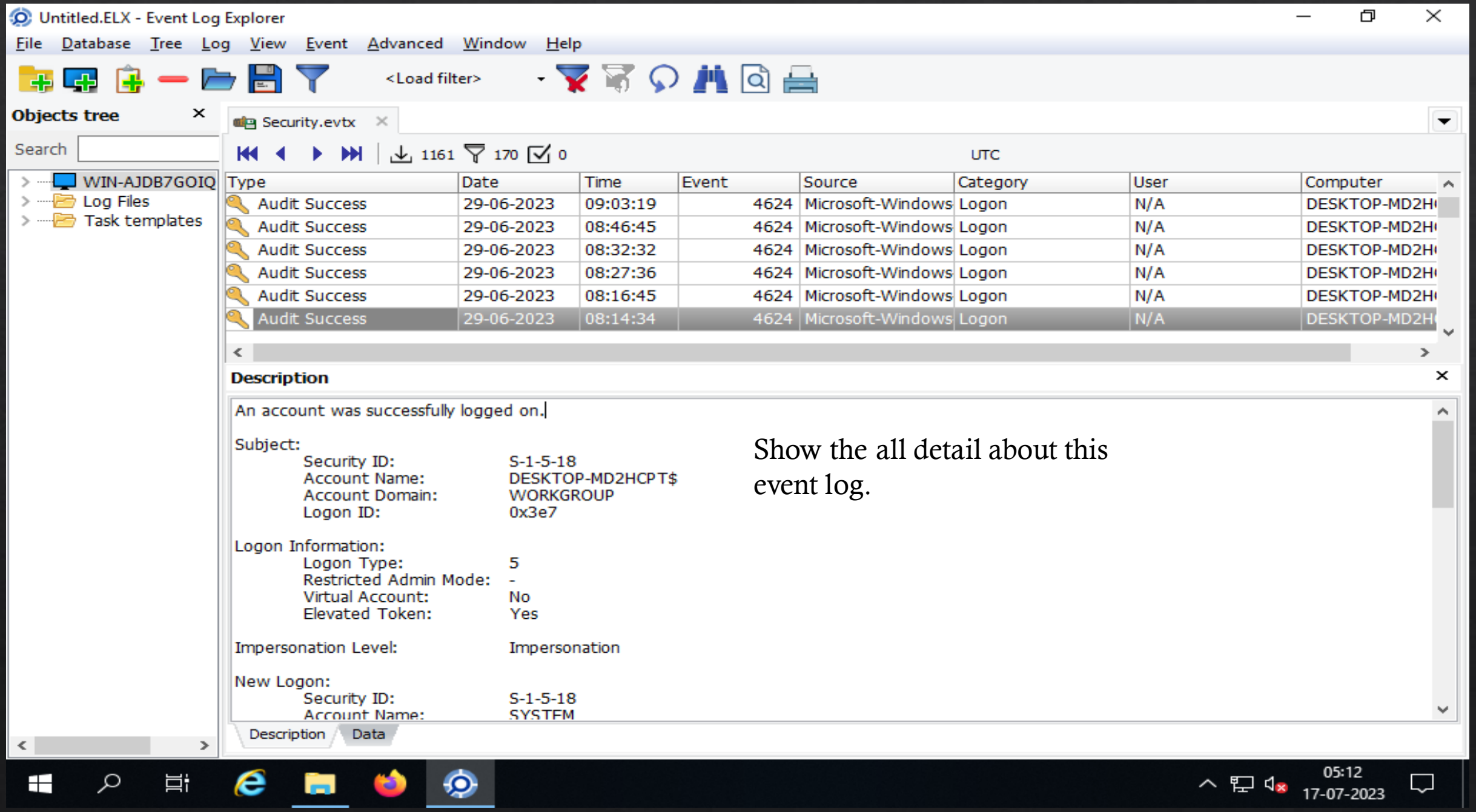
Click the security event log and load on the event explorer



Click this icon for filter the event id



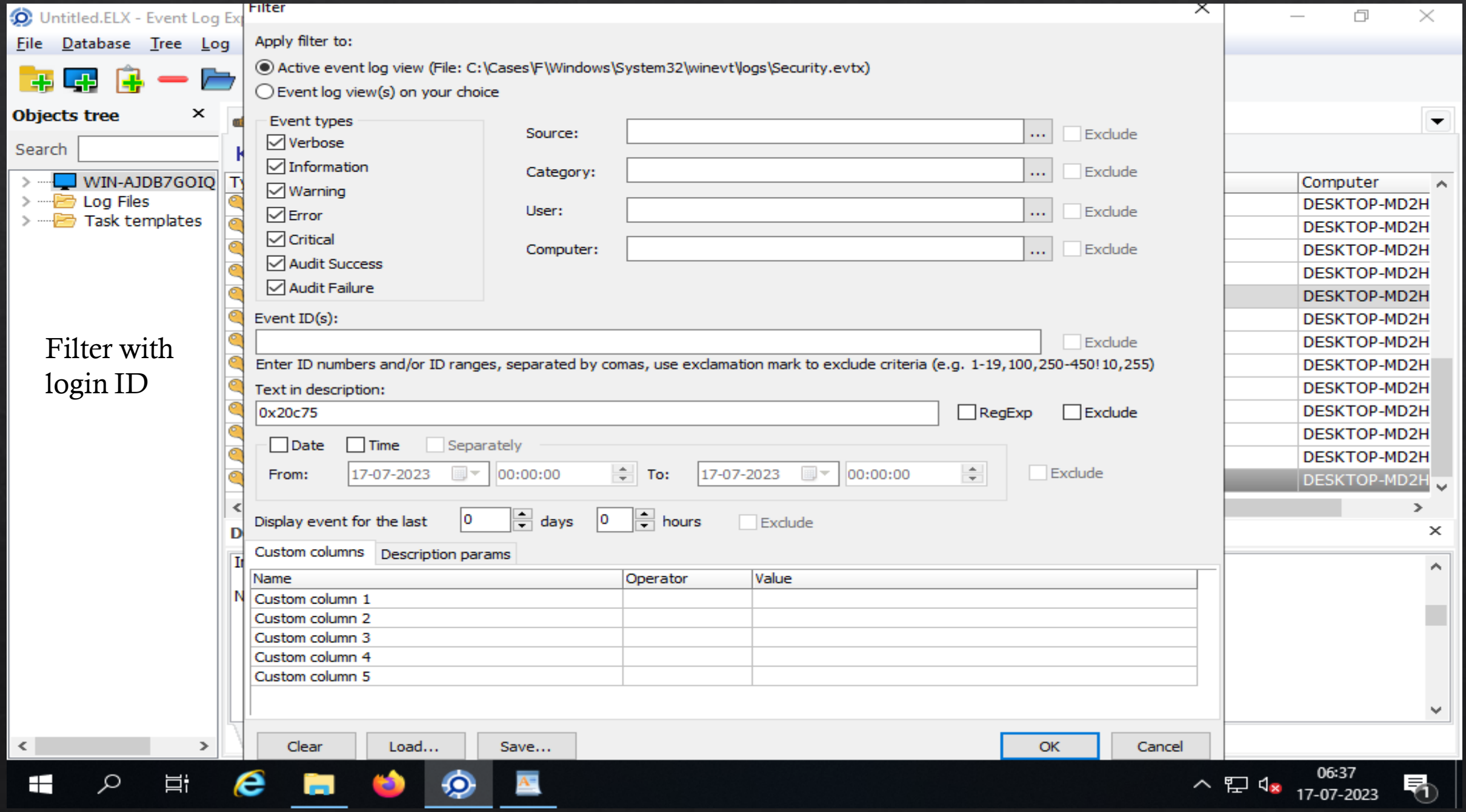
Fill the event id and description as per requirement

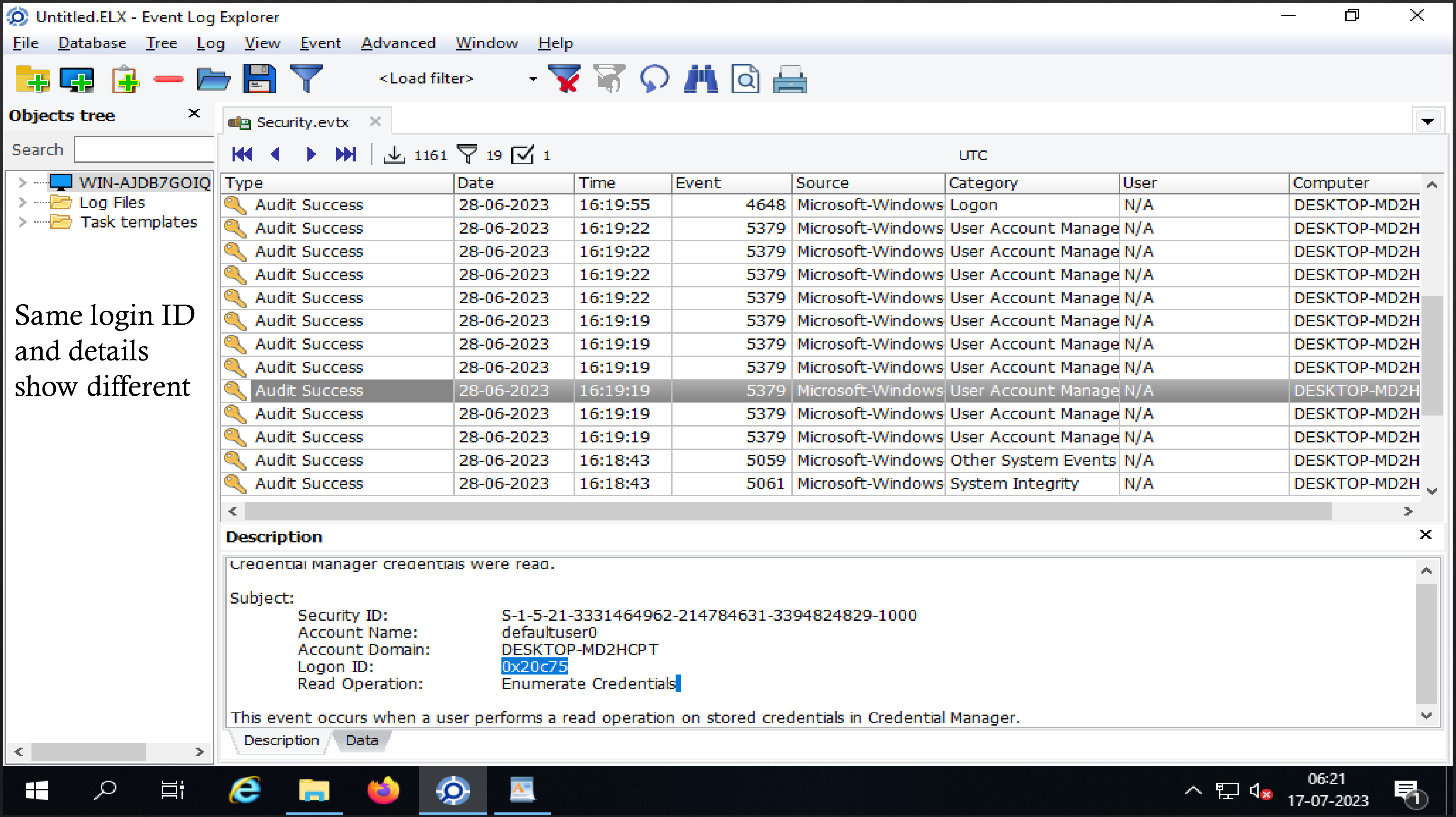


Show the all detail about this event log.

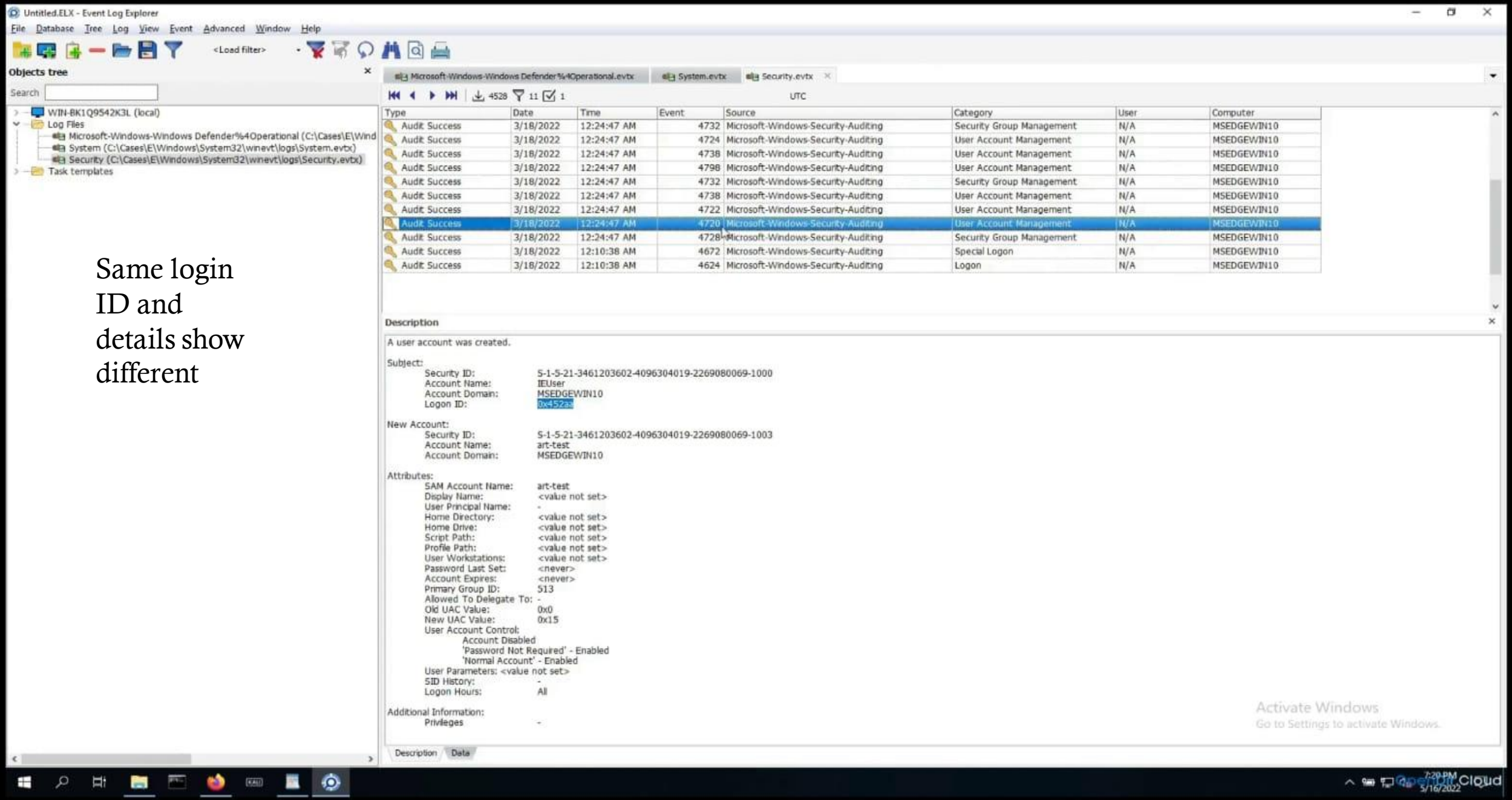
4. Authentication & Logon IDs logs

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 Ex
File Database Tree Log
Objects tree
Search
WIN-AJDB7GOIQ
Log Files
Task templates
Filter with login ID
Filter
Apply filter to:
Active event log view (File: C:\Cases\F\Windows\System32\winevt\logs\Security.evtx)
Event log view(s) on your choice
Event types
Verbose
Information
Warning
Error
Critical
Audit Success
Audit Failure
Source:
Category:
User:
Computer:
Exclude
Event ID(s):
Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)
Text in description:
0x20c75
RegExp
Date
Time
Separately
From:
17-07-2023
00:00:00
To:
Display event for the last
days
hours
Custom columns
Description params
Name
Operator
Value
Custom column 1
Custom column 2
Custom column 3
Custom column 4
Custom column 5
Clear
Load...
Save...
OK
Cancel
Computer
DESKTOP-MD2H
06:37
17-07-2023



Same login ID and details show different

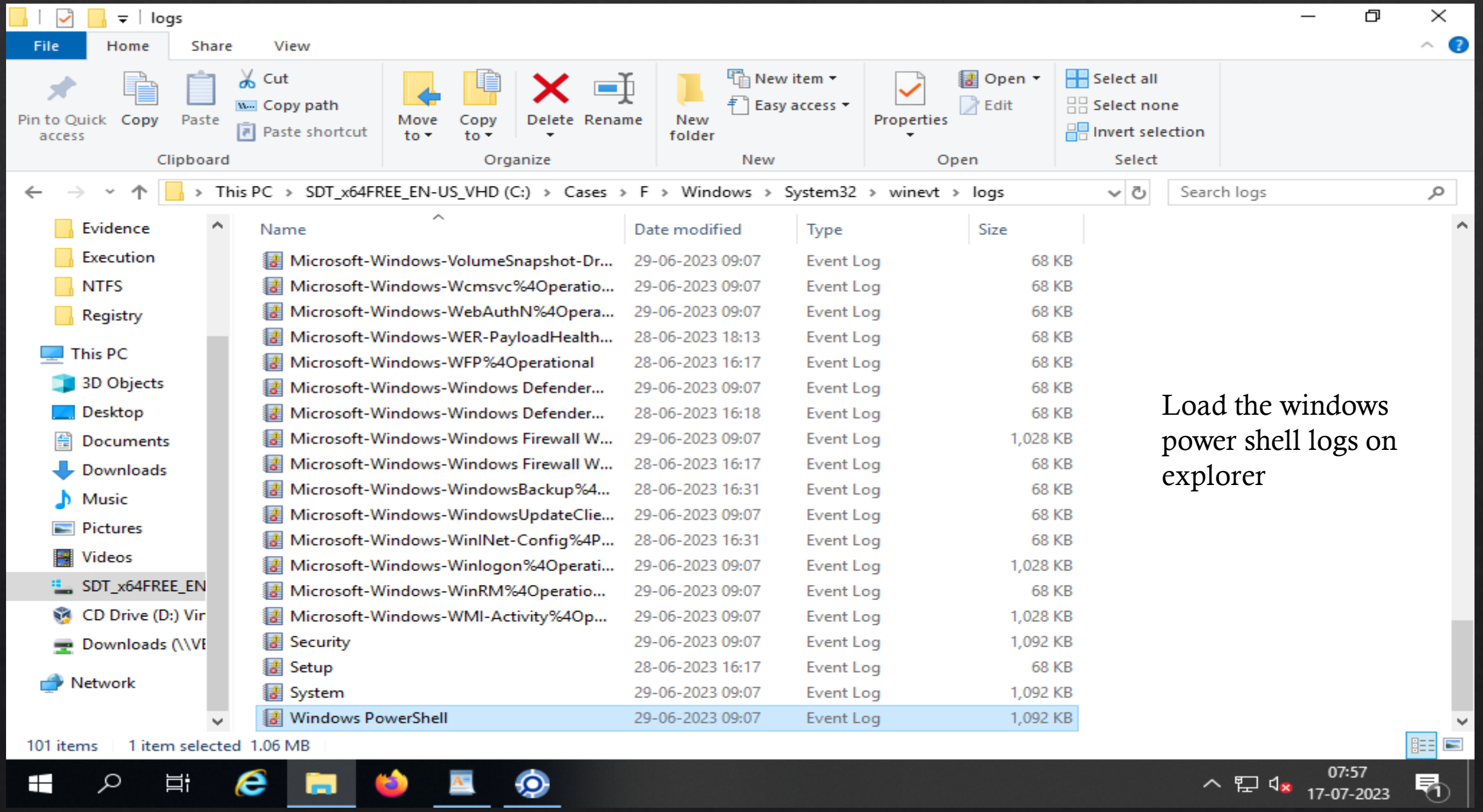


Same login ID and details show different

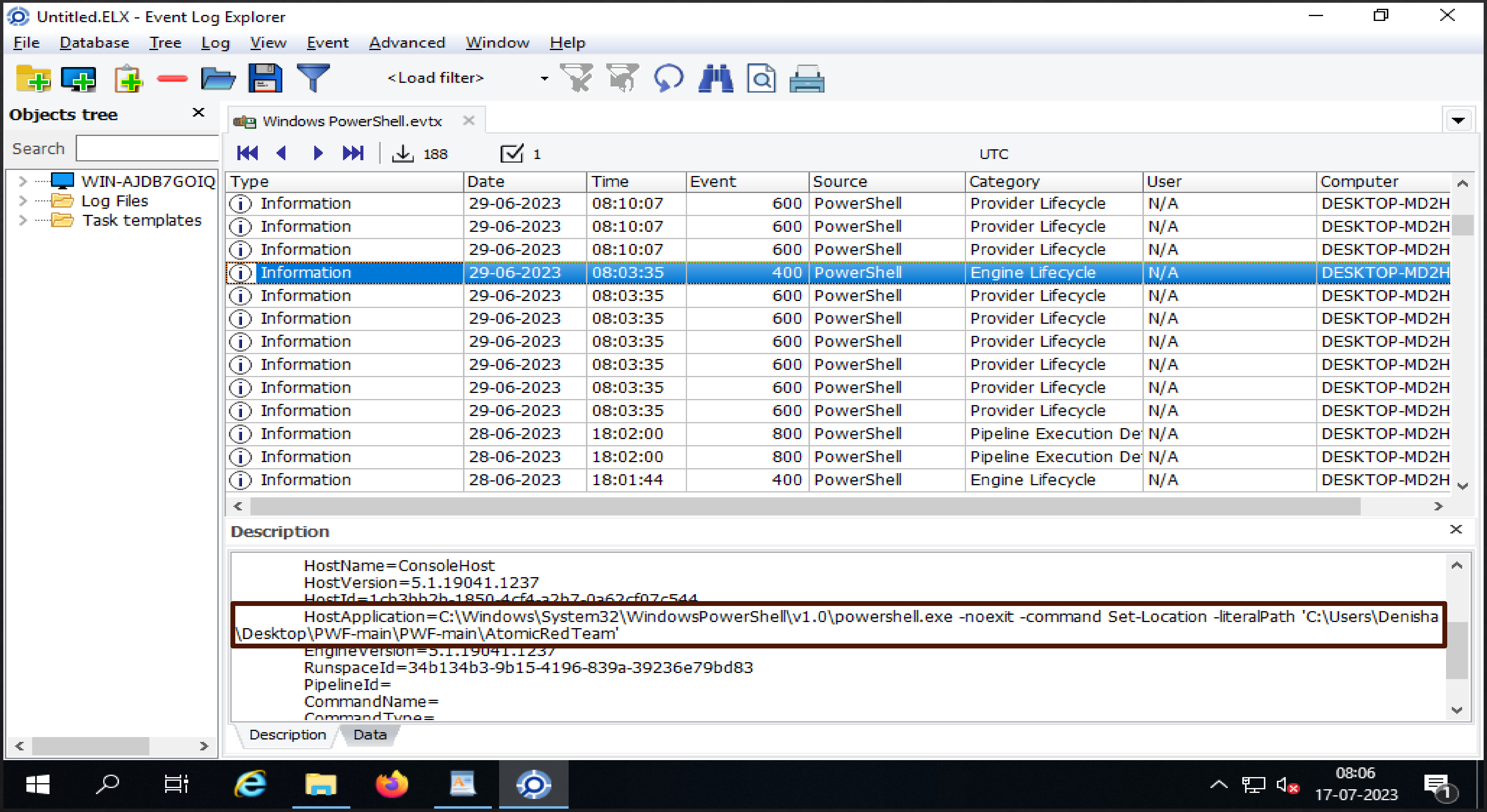
5. Windows Event logs Power shell overview,Analyse Malicious Activity.

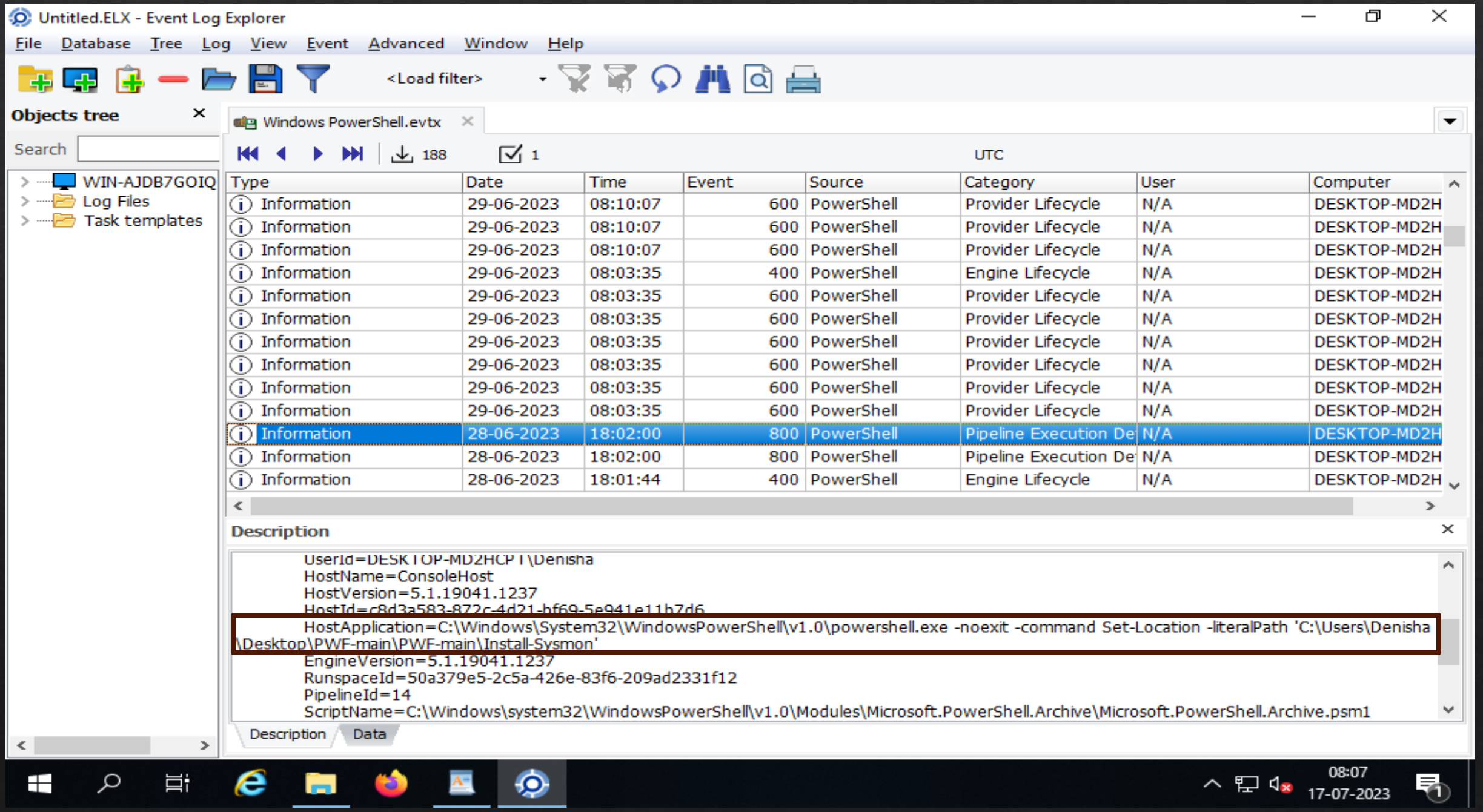
Source	Event IDs	Description
Windows PowerShell	400	Engine state is changed from None to Available

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



Load the windows power shell logs on explorer

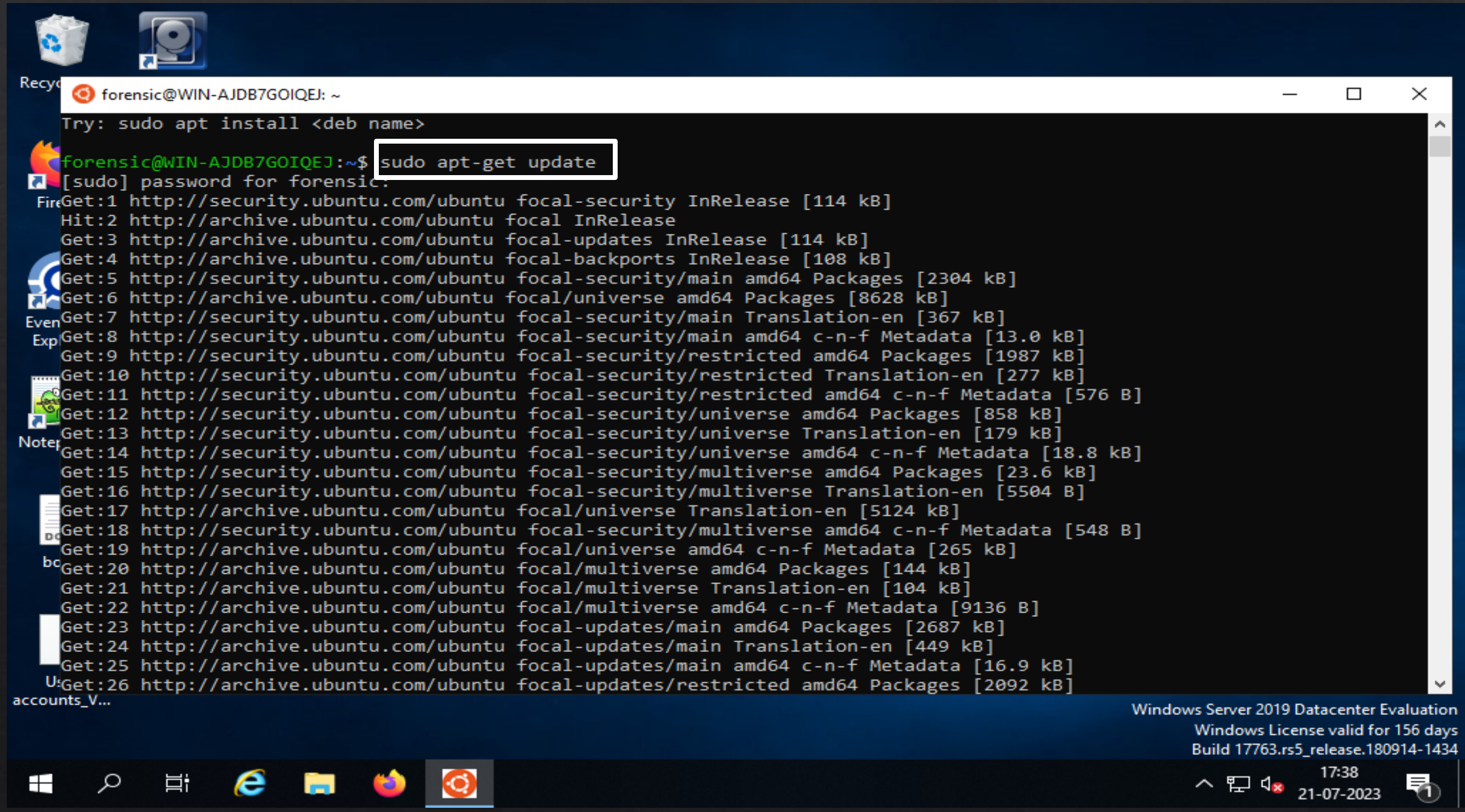

Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
<Load filter>
Objects tree
Search
WIN-AJDB7GOIQ
Log Files
Task templates
Windows PowerShell.evtx
188
1
UTC
Type Date Time Event Source Category User Computer
Information 29-06-2023 08:10:07 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:10:07 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:10:07 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 400 PowerShell Engine Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 28-06-2023 18:02:00 800 PowerShell Pipeline Execution De N/A DESKTOP-MD2H
Information 28-06-2023 18:02:00 800 PowerShell Pipeline Execution De N/A DESKTOP-MD2H
Information 28-06-2023 18:01:44 400 PowerShell Engine Lifecycle N/A DESKTOP-MD2H
Description
HostName=ConsoleHost
HostVersion=5.1.19041.1237
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noexit -command Set-Location -literalPath 'C:\Users\Denisha\Desktop\PWF-main\PWF-main\AtomicRedTeam'
RunspaceId=34b134b3-9b15-4196-839a-39236e79bd83
PipelineId=
CommandName=
Description Data
08:06
17-07-2023

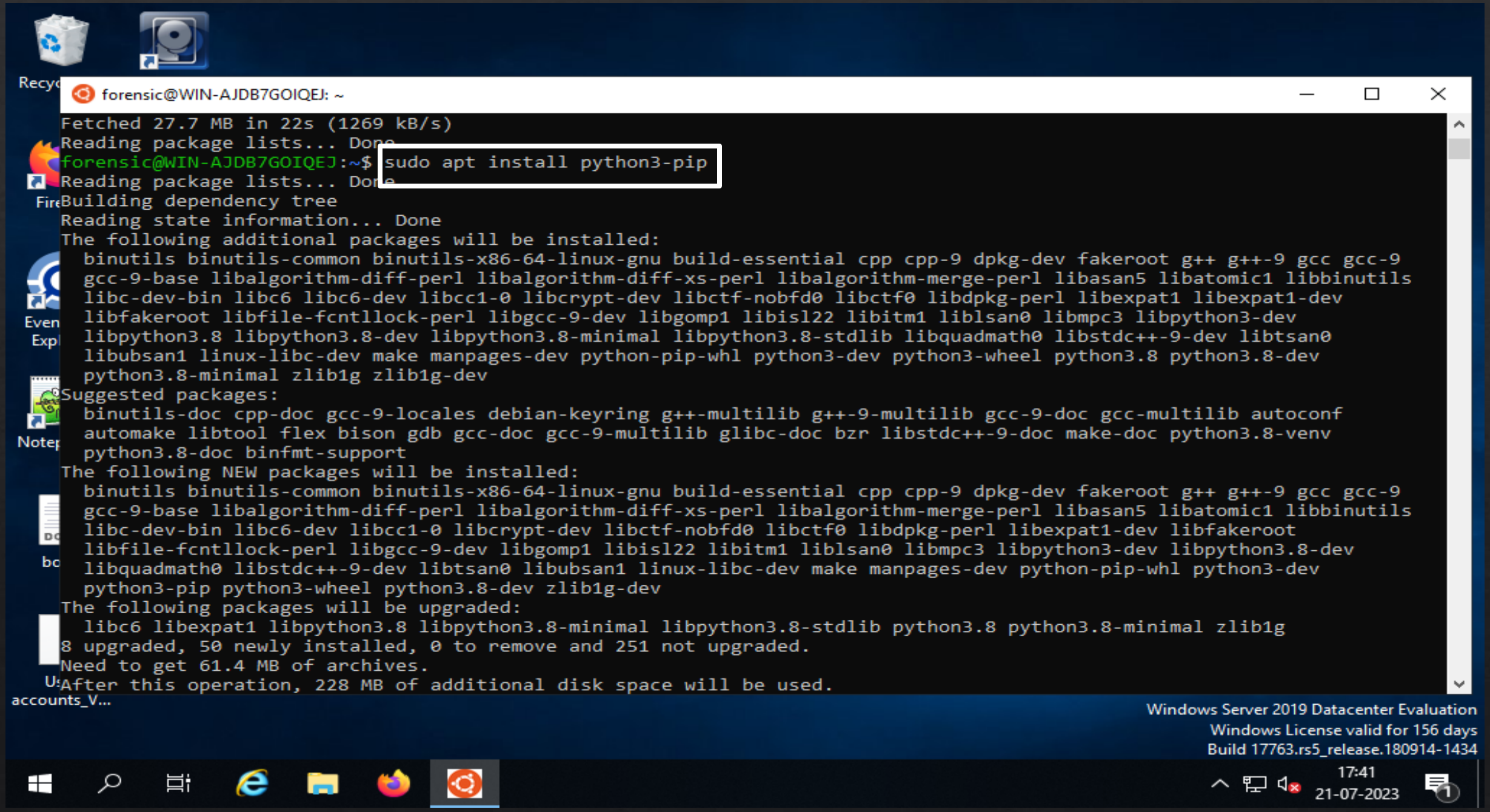

Untitled.ELX - Event Log Explorer
File Database Tree Log View Event Advanced Window Help
<Load filter>
Objects tree
Search
WIN-AJDB7GOIQ
Log Files
Task templates
Windows PowerShell.evtx
188
1
UTC
Type Date Time Event Source Category User Computer
Information 29-06-2023 08:10:07 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:10:07 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:10:07 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 400 PowerShell Engine Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 29-06-2023 08:03:35 600 PowerShell Provider Lifecycle N/A DESKTOP-MD2H
Information 28-06-2023 18:02:00 800 PowerShell Pipeline Execution De N/A DESKTOP-MD2H
Information 28-06-2023 18:02:00 800 PowerShell Pipeline Execution De N/A DESKTOP-MD2H
Information 28-06-2023 18:01:44 400 PowerShell Engine Lifecycle N/A DESKTOP-MD2H
Description
UserId=DESKTOP-MD2HCPT\Denisha
HostName=ConsoleHost
HostVersion=5.1.19041.1237
HostId=c8d3a583-872c-4d21-bf69-5e941e11b7d6
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noexit -command Set-Location -literalPath 'C:\Users\Denisha\Desktop\PWF-main\PWF-main\Install-Sysmon'
EngineVersion=5.1.19041.1237
RunspaceId=50a379e5-2c5a-426e-83f6-209ad2331f12
PipelineId=14
ScriptName=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psm1
Description Data
08:07
17-07-2023

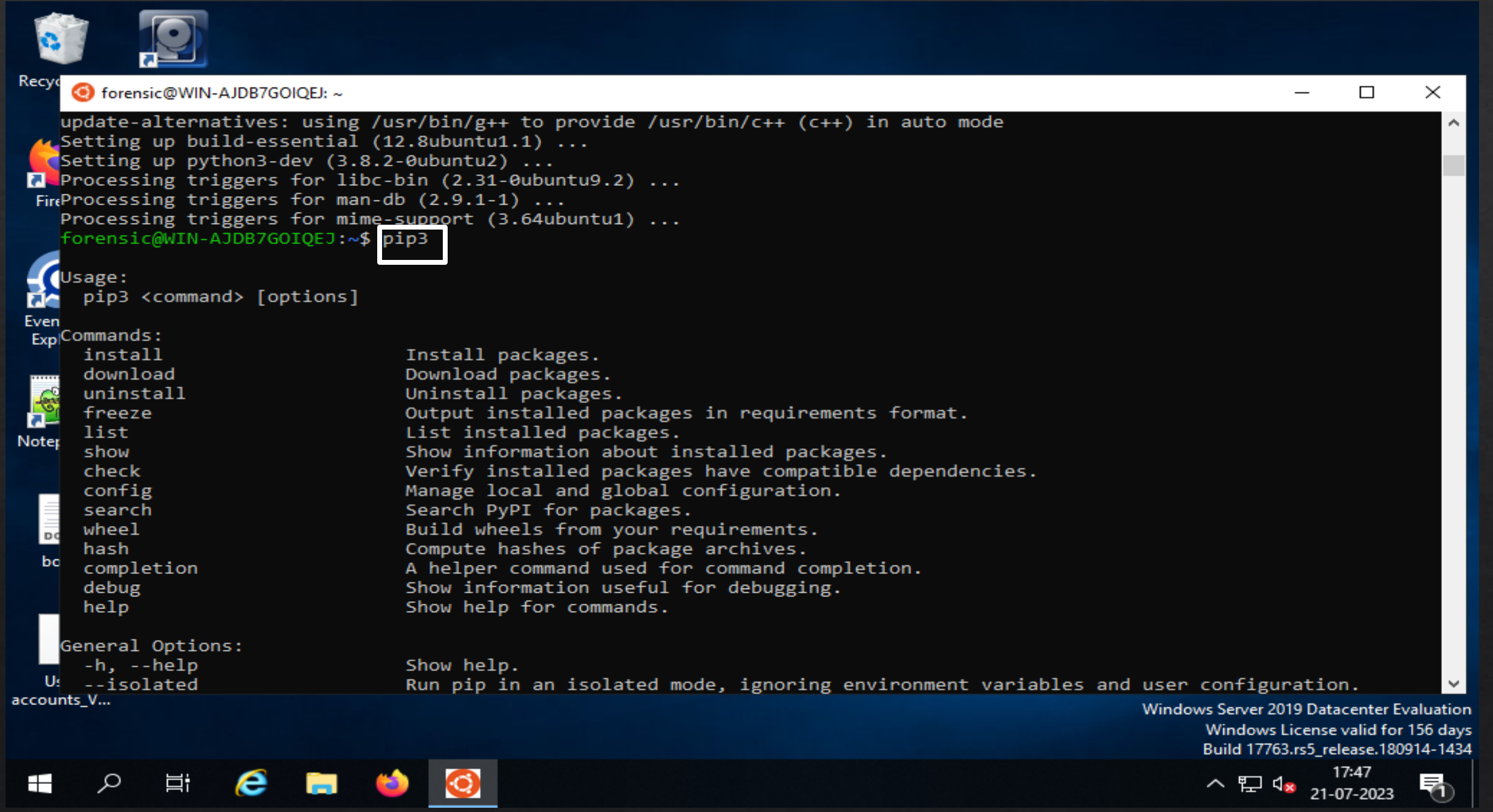
Memory Analysis

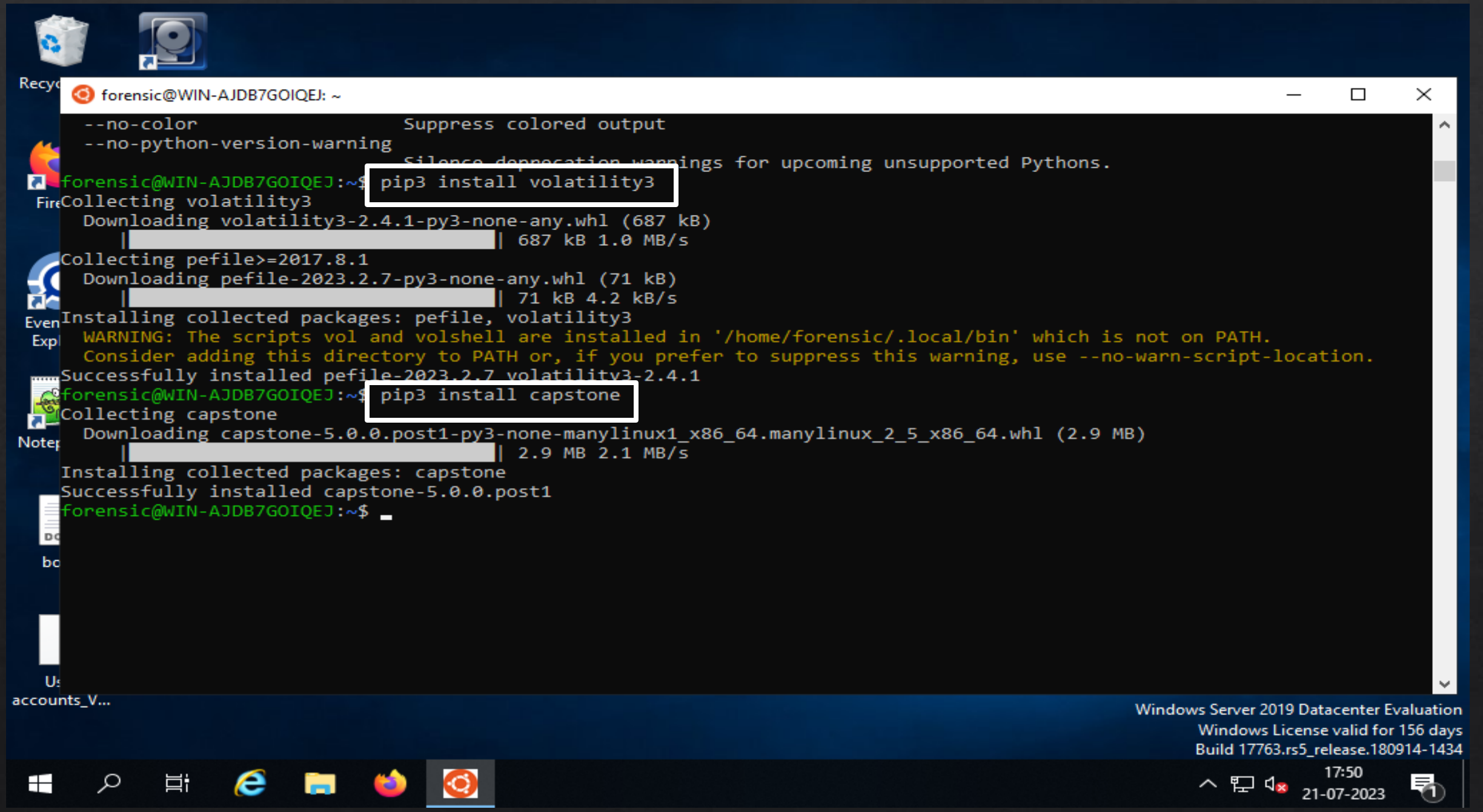
Setting up volatility3 in Ubuntu

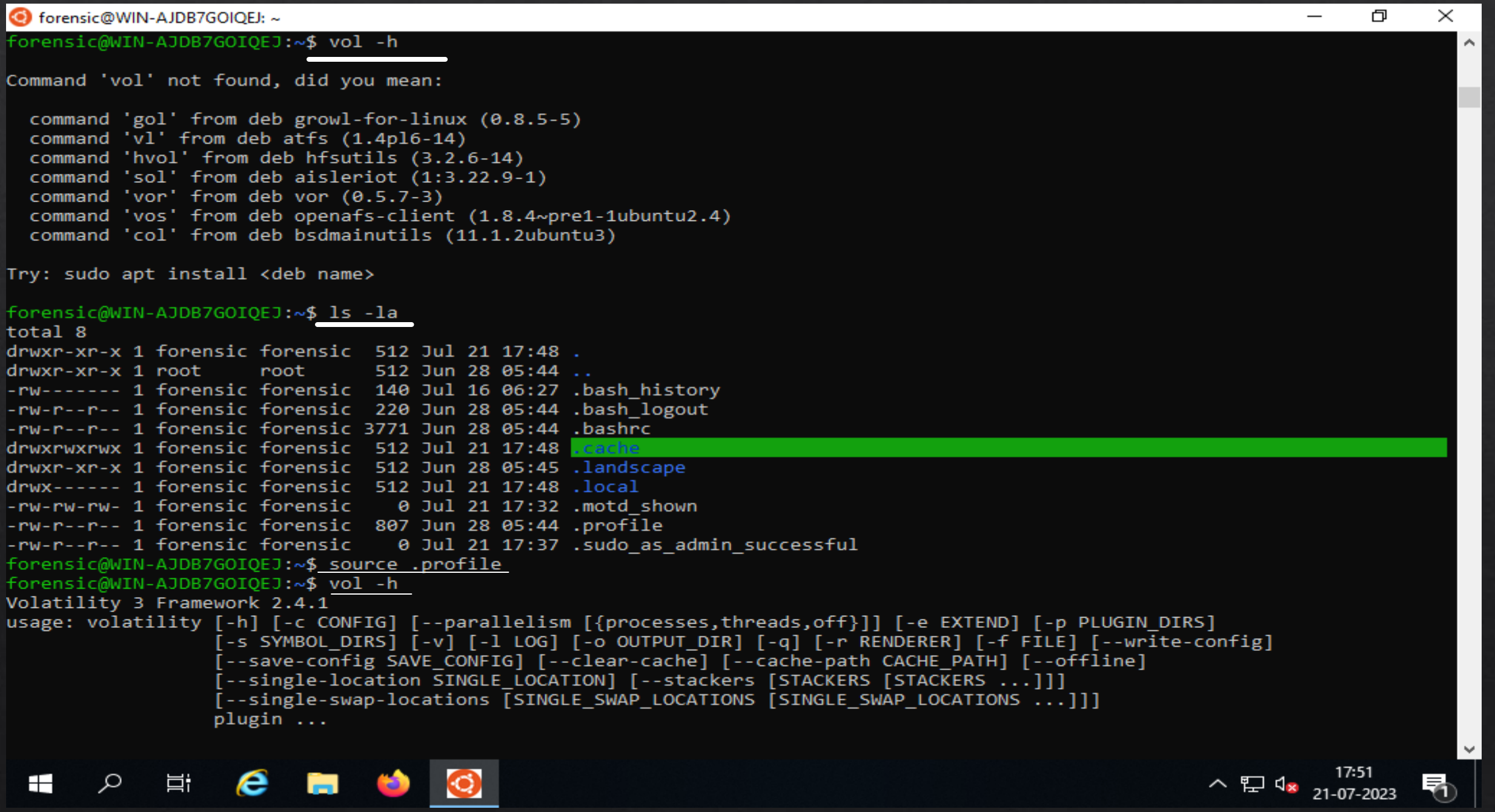
Setting up the Volatility3 in the Ubuntu that open the link https://bluecapesecurity.com/build-your-forensic-workstation/
Show the instruction linux based tools.


forensic@WIN-AJDB7GOIQEJ: ~
Try: sudo apt install <deb name>
forensic@WIN-AJDB7GOIQEJ:~$ sudo apt-get update
[sudo] password for forensic:
Get:1 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Hit:2 http://archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:5 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [2304 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal/universe amd64 Packages [8628 kB]
Get:7 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [367 kB]
Get:8 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [13.0 kB]
Get:9 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [1987 kB]
Get:10 http://security.ubuntu.com/ubuntu focal-security/restricted Translation-en [277 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 c-n-f Metadata [576 B]
Get:12 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [858 kB]
Get:13 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [179 kB]
Get:14 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [18.8 kB]
Get:15 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Packages [23.6 kB]
Get:16 http://security.ubuntu.com/ubuntu focal-security/multiverse Translation-en [5504 B]
Get:17 http://archive.ubuntu.com/ubuntu focal/universe Translation-en [5124 kB]
Get:18 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 c-n-f Metadata [548 B]
Get:19 http://archive.ubuntu.com/ubuntu focal/universe amd64 c-n-f Metadata [265 kB]
Get:20 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [144 kB]
Get:21 http://archive.ubuntu.com/ubuntu focal/multiverse Translation-en [104 kB]
Get:22 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 c-n-f Metadata [9136 B]
Get:23 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [2687 kB]
Get:24 http://archive.ubuntu.com/ubuntu focal-updates/main Translation-en [449 kB]
Get:25 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [16.9 kB]
Get:26 http://archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [2092 kB]
accounts_V...
Windows Server 2019 Datacenter Evaluation
Windows License valid for 156 days
Build 17763.rs5_release.180914-1434
17:38
21-07-2023


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


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

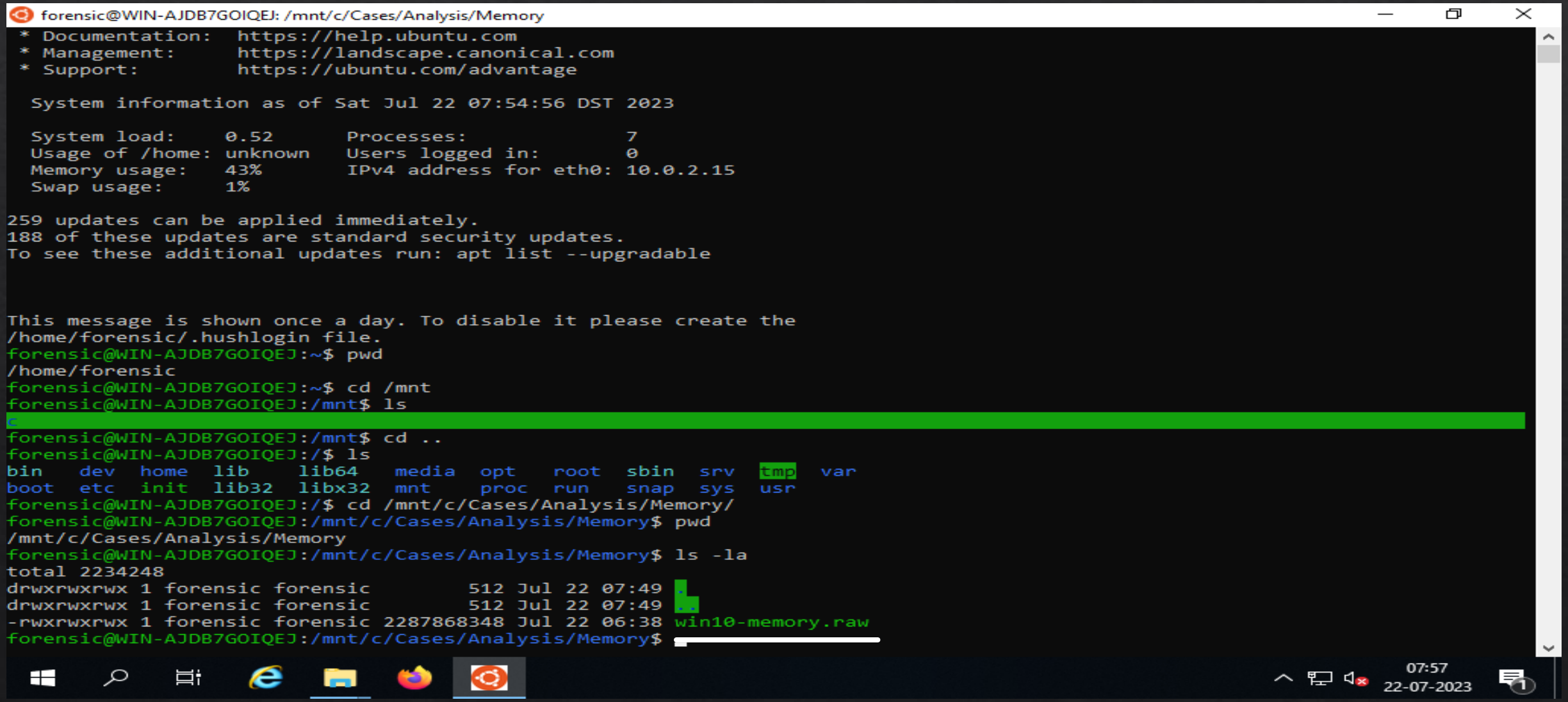

forensic@WIN-AJDB7GOIQEJ: ~
--no-color Suppress colored output
--no-python-version-warning
Silence deprecation warnings for upcoming unsupported Pythons.
forensic@WIN-AJDB7GOIQEJ:~$ pip3 install volatility3
Collecting volatility3
Downloading volatility3-2.4.1-py3-none-any.whl (687 kB)
| 687 kB 1.0 MB/s
Collecting pefile>=2017.8.1
Downloading pefile-2023.2.7-py3-none-any.whl (71 kB)
| 71 kB 4.2 kB/s
Installing collected packages: pefile, volatility3
WARNING: The scripts vol and volshell are installed in '/home/forensic/.local/bin' which is not on PATH.
Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed pefile-2023.2.7 volatility3-2.4.1
forensic@WIN-AJDB7GOIQEJ:~$ pip3 install capstone
Collecting capstone
Downloading capstone-5.0.0.post1-py3-none-manylinux1_x86_64.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:~$
Windows Server 2019 Datacenter Evaluation
Windows License valid for 156 days
Build 17763.rs5_release.180914-1434
17:50
21-07-2023


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

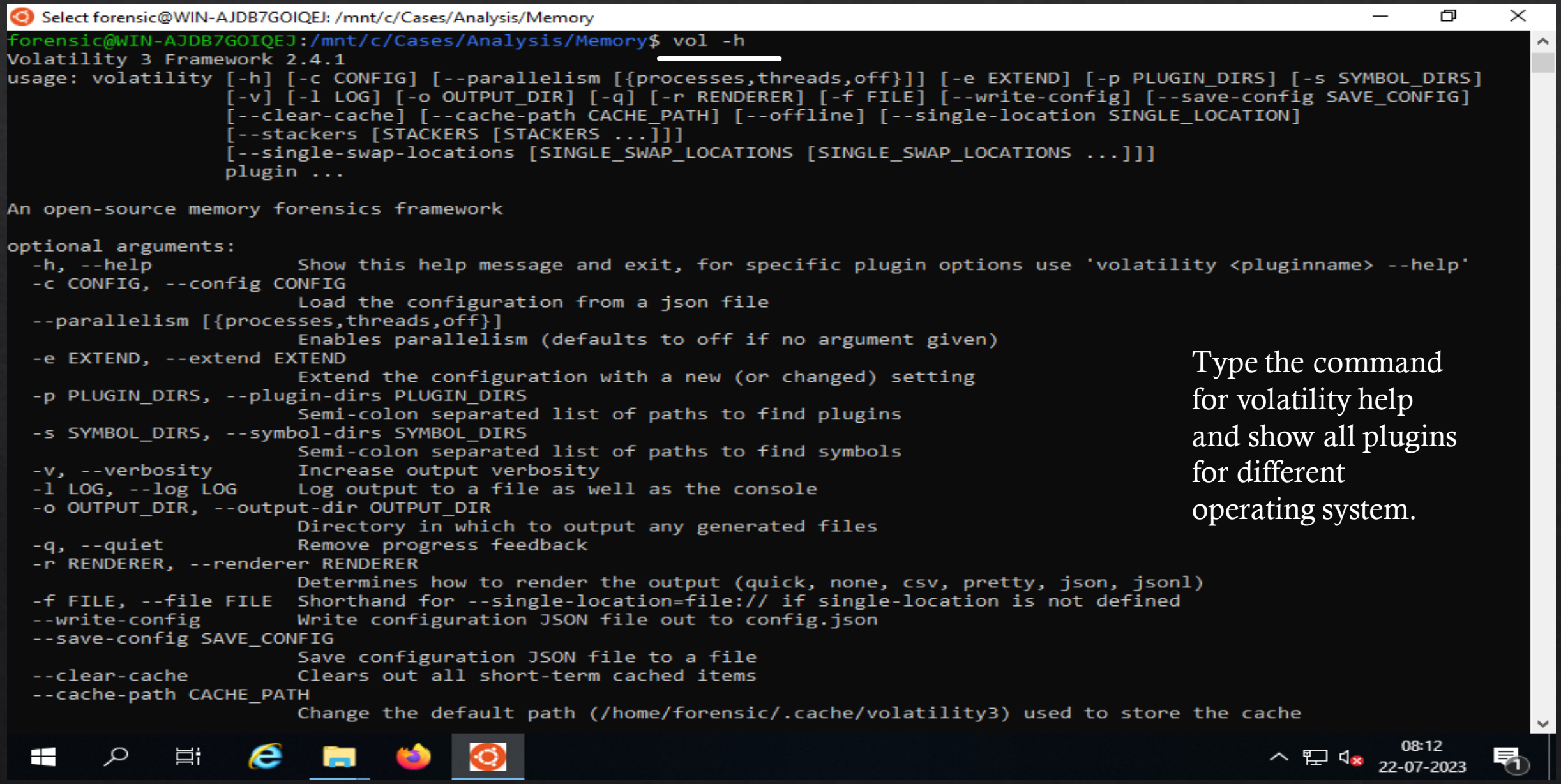
What is memory Analysis

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.



Gathering Windows system information with Volatility3



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

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 .

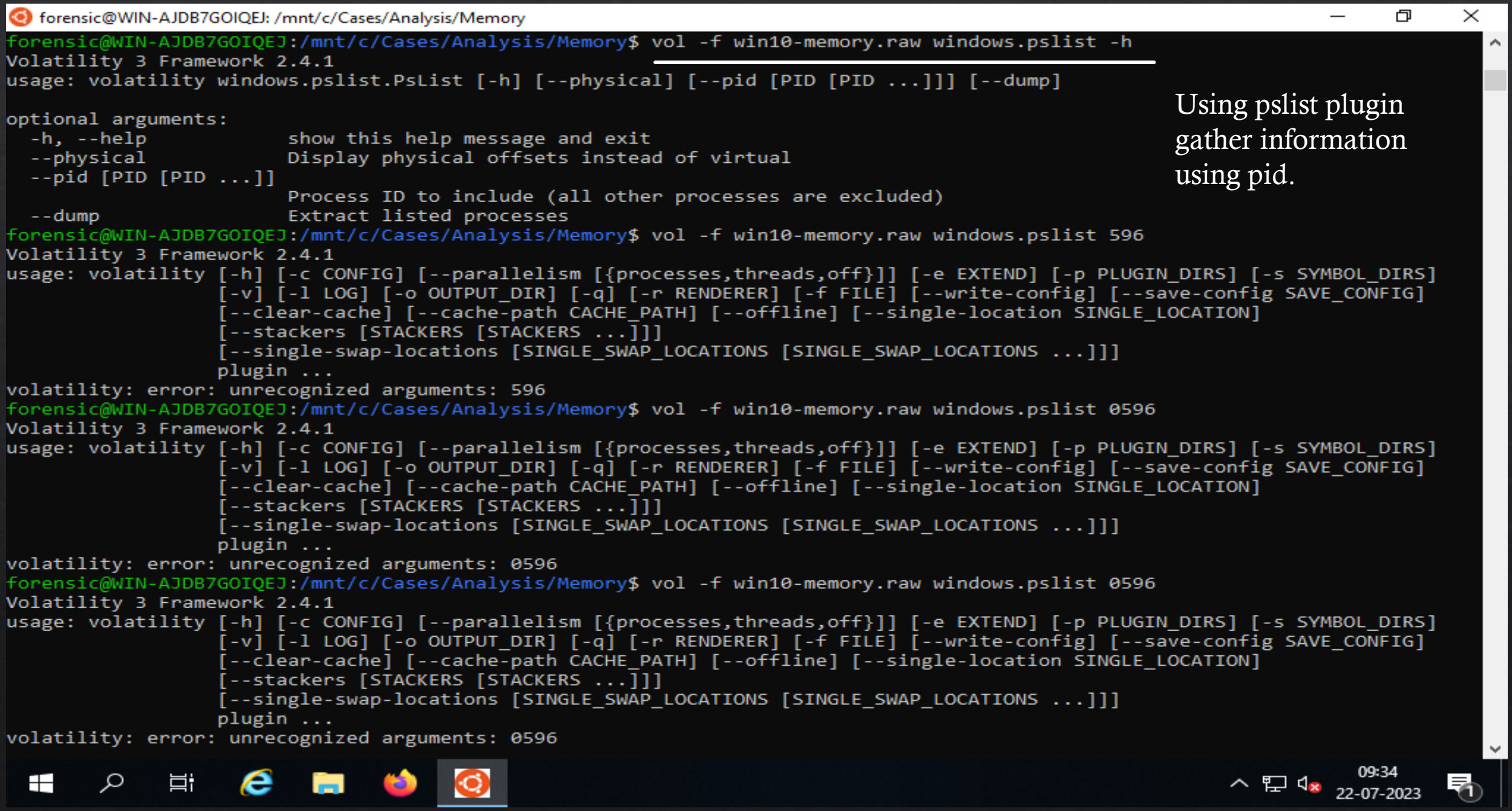
forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/Memory

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

Variable        Value

Kernel Base     0xf8063d41d000
DTB     0x1aa000
Symbols file:///home/forensic/.local/lib/python3.8/site-packages/volatility3/symbols/windows/ntkrnlmp.pdb/CA8E2F01B822EDE6357
898BFBF862997-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 Elf64Layer
base_layer      2 FileLayer
KdVersionBlock  0xf8063e02c368
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      2
SystemTime      2023-07-22 06:37:29
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Wed Jan  4 04:27:11 1995
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.info
```

Type this command how the result.

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

```
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 TimeDateStamp        Wed Jan  4 04:27:11 1995
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pstree
Volatility 3 Framework 2.4.1
^Z^Cress:   11.38               Scanning memory_layer using BytesScanner
[1]+  Stopped                 vol -f win10-memory.raw windows.pstree
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pstree > pstree.txt
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pstree
Volatility 3 Framework 2.4.1
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0xcc068767d080  124     -       N/A     False   2023-07-22 06:33:09.000000      N/A
* 1404  4       MemCompression  0xcc068e308040  14      -       N/A     False   2023-07-22 06:34:20.000000      N/A
* 92    4       Registry        0xcc06877b6040  4       -       N/A     False   2023-07-22 06:30:52.000000      N/A
* 348   4       smss.exe        0xcc0687c6c040  2       -       N/A     False   2023-07-22 06:33:09.000000      N/A
532     512     csrss.exe       0xcc068d369080  12      -       1       False   2023-07-22 06:33:37.000000      N/A
596     512     winlogon.exe    0xcc068a750240  6       -       1       False   2023-07-22 06:33:37.000000      N/A
* 800   596     fontdrvhost.ex  0xcc068d3f6080  5       -       1       False   2023-07-22 06:33:40.000000      N/A
* 2180  596     userinit.exe    0xcc068eaaf080  0       -       1       False   2023-07-22 06:36:41.000000      2023-07-22 06
:36:56.000000
** 2488 2180    explorer.exe    0xcc068ec78080  49      -       1       False   2023-07-22 06:36:43.000000      N/A
* 976   596     dwm.exe 0xcc068e14a300  16      -       1       False   2023-07-22 06:33:42.000000      N/A
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$
```



Using pslist plugin gather information using pid.

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

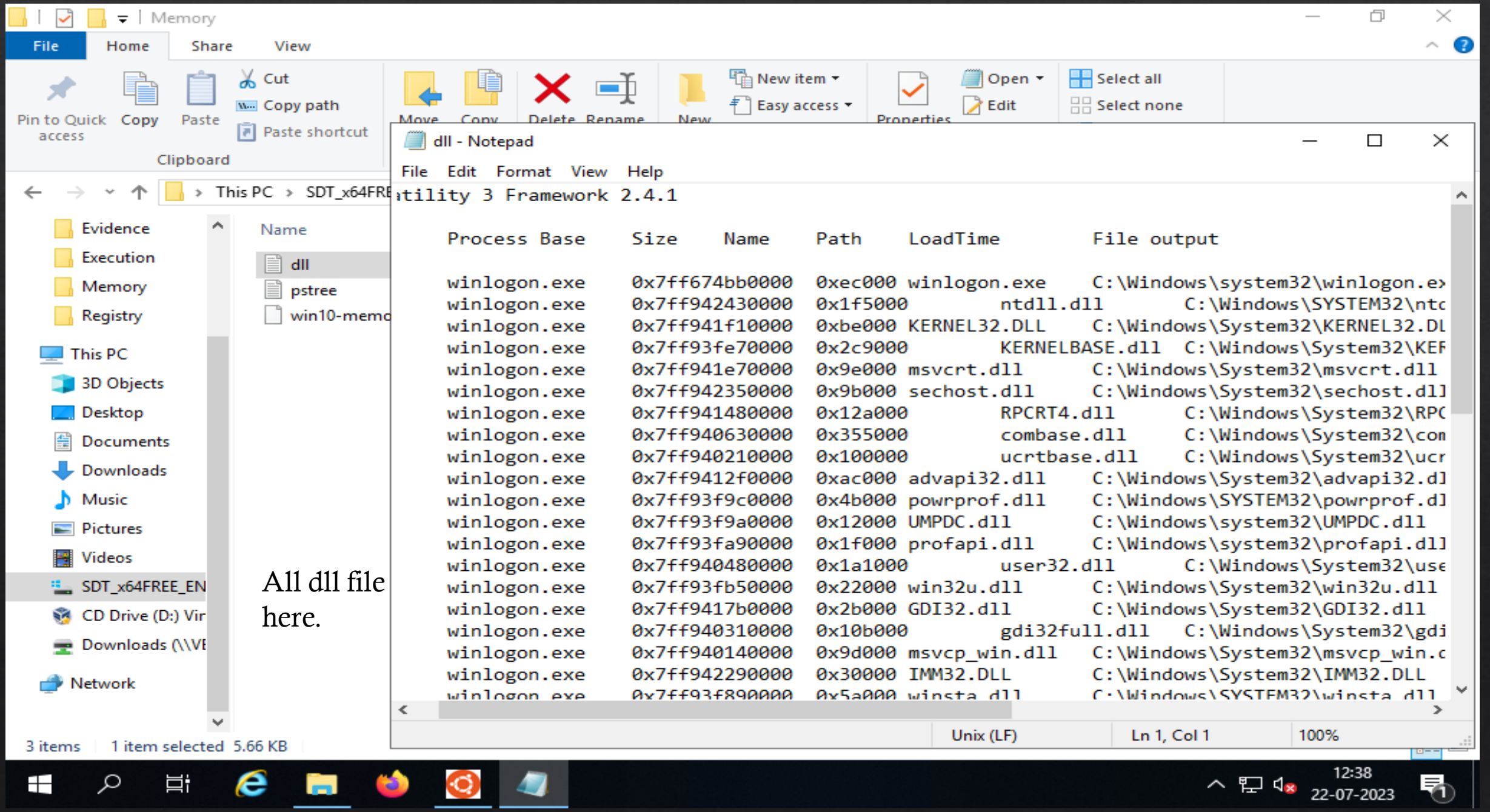
```
                [--stackers [STACKERS [STACKERS ...]]]
                [--single-swap-locations [SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_LOCATIONS ...]]]
                plugin ...
volatility: error: unrecognized arguments: 596
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw 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

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$
```

Show the services for individual pid

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$
```

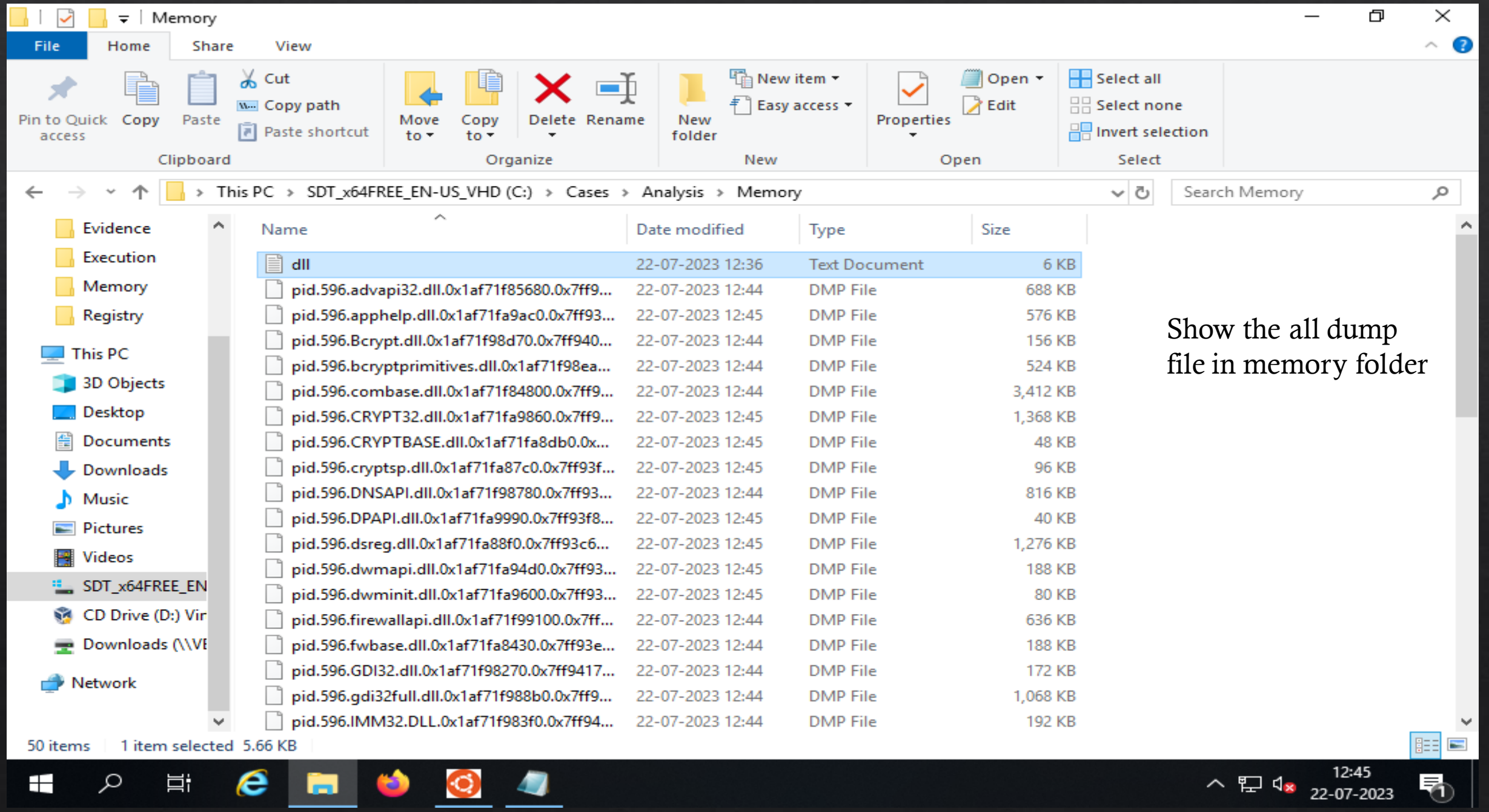
Search other files run on pid no 596 using dll list.


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
This PC
SDT_x64FRE
Evidence
Execution
Memory
Registry
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
SDT_x64FREE_EN
CD Drive (D:) Vir
Downloads (\\VE
Network
Name
dll
pstree
win10-memo
All dll file here.
3 items
1 item selected 5.66 KB
dll - Notepad
File Edit Format View Help
tility 3 Framework 2.4.1
Process Base Size Name Path LoadTime File output
winlogon.exe 0x7ff674bb0000 0xec000 winlogon.exe C:\Windows\system32\winlogon.ex
winlogon.exe 0x7ff942430000 0x1f5000 ntdll.dll C:\Windows\SYSTEM32\ntc
winlogon.exe 0x7ff941f10000 0xbe000 KERNEL32.DLL C:\Windows\System32\KERNEL32.DL
winlogon.exe 0x7ff93fe70000 0x2c9000 KERNELBASE.dll C:\Windows\System32\KEF
winlogon.exe 0x7ff941e70000 0x9e000 msvcrt.dll C:\Windows\System32\msvcrt.dll
winlogon.exe 0x7ff942350000 0x9b000 sechost.dll C:\Windows\System32\sechost.dll
winlogon.exe 0x7ff941480000 0x12a000 RPCRT4.dll C:\Windows\System32\RPC
winlogon.exe 0x7ff940630000 0x355000 combase.dll C:\Windows\System32\com
winlogon.exe 0x7ff940210000 0x100000 ucrtbase.dll C:\Windows\System32\ucr
winlogon.exe 0x7ff9412f0000 0xac000 advapi32.dll C:\Windows\System32\advapi32.dl
winlogon.exe 0x7ff93f9c0000 0x4b000 powrprof.dll C:\Windows\SYSTEM32\powrprof.dl
winlogon.exe 0x7ff93f9a0000 0x12000 UMPDC.dll C:\Windows\system32\UMPDC.dll
winlogon.exe 0x7ff93fa90000 0x1f000 profapi.dll C:\Windows\system32\profapi.dll
winlogon.exe 0x7ff940480000 0x1a1000 user32.dll C:\Windows\System32\use
winlogon.exe 0x7ff93fb50000 0x22000 win32u.dll C:\Windows\System32\win32u.dll
winlogon.exe 0x7ff9417b0000 0x2b000 GDI32.dll C:\Windows\System32\GDI32.dll
winlogon.exe 0x7ff940310000 0x10b000 gdi32full.dll C:\Windows\System32\gdi
winlogon.exe 0x7ff940140000 0x9d000 msvcp_win.dll C:\Windows\System32\msvcp_win.c
winlogon.exe 0x7ff942290000 0x30000 IMM32.DLL C:\Windows\System32\IMM32.DLL
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
PID     Process Base    Size    Name    Path    LoadTime        File output

596     winlogon.exe    0x7ff674bb0000  0xec000 winlogon.exe    C:\Windows\system32\winlogon.exe        2023-07-22 06:33:37.0
00000   pid.596.winlogon.exe.0x1af71f81e90.0x7ff674bb0000.dmp
596     winlogon.exe    0x7ff942430000  0x1f5000        ntdll.dll       C:\Windows\SYSTEM32\ntdll.dll   2023-07-22 06:33:37.0
00000   pid.596.ntdll.dll.0x1af71f81d00.0x7ff942430000.dmp
596     winlogon.exe    0x7ff941f10000  0xbe000 KERNEL32.DLL    C:\Windows\System32\KERNEL32.DLL        2023-07-22 06:33:37.0
00000   pid.596.KERNEL32.DLL.0x1af71f82430.0x7ff941f10000.dmp
596     winlogon.exe    0x7ff93fe70000  0x2c9000        KERNELBASE.dll  C:\Windows\System32\KERNELBASE.dll      2023-07-22 06
:33:37.000000   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   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
```

Extract the files and give more information



Show the all dump file in memory folder

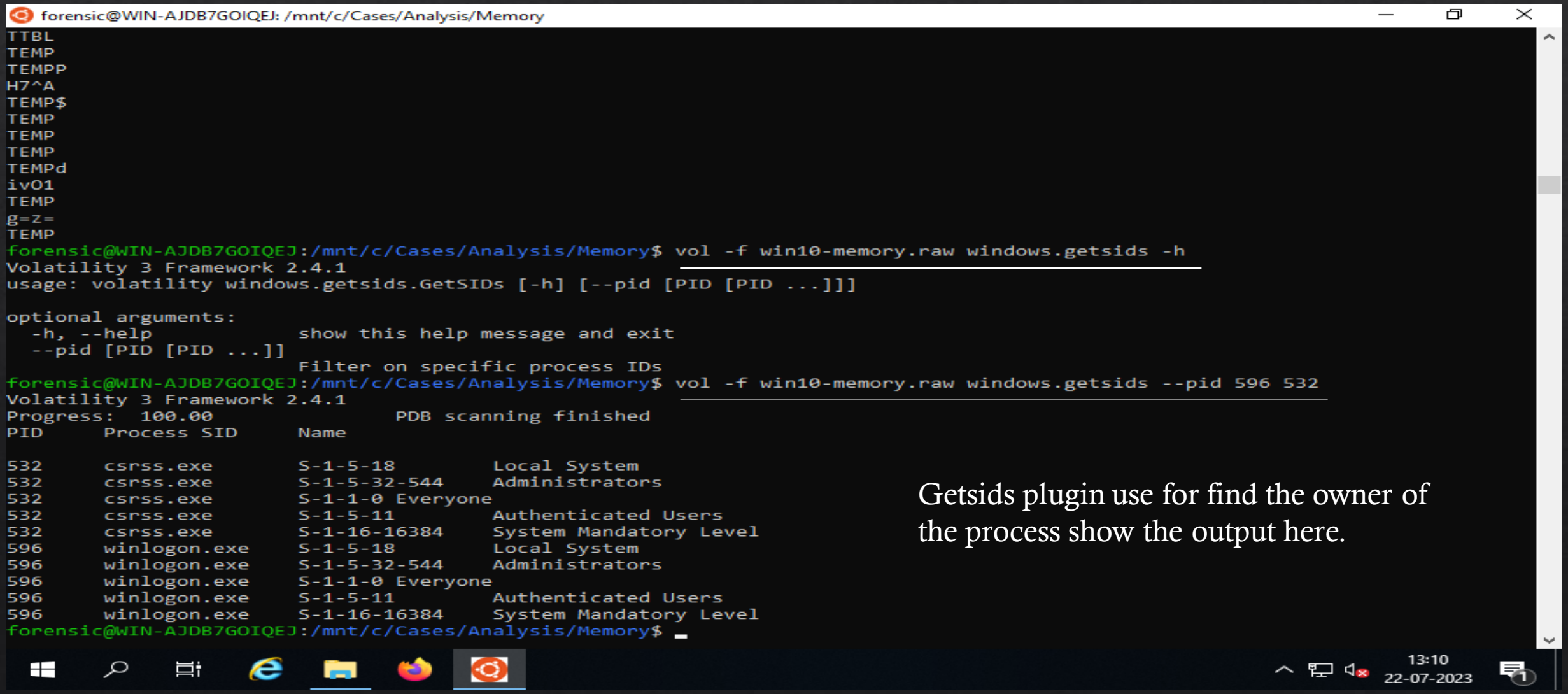
Select forensic@WIN-AJDB7GOIQEJ: /mnt/c/Cases/Analysis/Memory

```
96.MPR.dll.0x1af71faa0b0.0x7ff939b60000.dmp
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ strings pid.596.dsreg.dll.0x1af71fa88f0.0x7ff93c680000.dmp
!This program cannot be run in DOS mode.
Rich8
.text
`.rdata
@.data
.pdata
@.didat
.rsrc
@.reloc
L$0H
L$xH
L$(H
D$0H
D$ H
L$0H3
\$XH
t$`H
T$xL
D$0A
D$4I
D$8H
D$ H
t$ UWAVH
f9<Bu
fA9<@u
fA9<@u
D$`H
D$PH
D$0L
D$pE3
L$xI
|$|H
M@H3
A^_]
t$ UWAWH
```

Gathering deep information using particular dmp file.

Identify process owners and associated SIDs

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

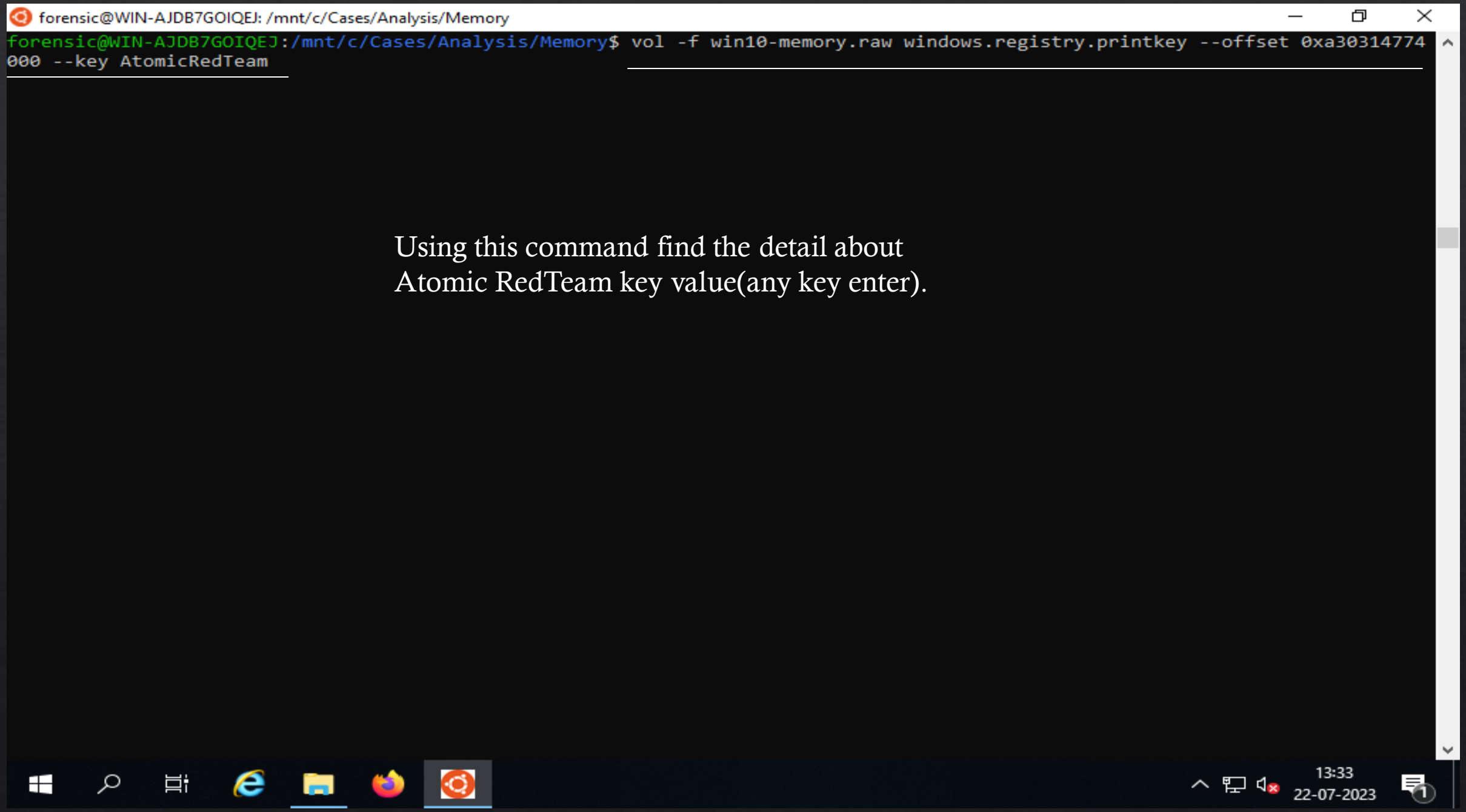


Getsids plugin use for find the owner of the process show the output here.

Detecting and Analyzing malicious registry key entries from memory

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

optional arguments:
  -h, --help       show this help message and exit
  --offset OFFSET  Hive Offset
  --key KEY        Key to start from
  --recurse        Recurses through keys
forensic@WIN-AJDB7GOIQEJ:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.registry.hivelist
Volatility 3 Framework 2.4.1
Progress:  100.00               PDB scanning finished
Offset  FileFullPath    File output

0xa3030e855000          Disabled
0xa3030e898000  \REGISTRY\MACHINE\SYSTEM        Disabled
0xa3030e8f1000  \REGISTRY\MACHINE\HARDWARE      Disabled
0xa303105e5000  \SystemRoot\System32\Config\SAM Disabled
0xa30310551000  \SystemRoot\System32\Config\SECURITY    Disabled
0xa303105f1000  \SystemRoot\System32\Config\DEFAULT     Disabled
0xa303105e7000  \SystemRoot\System32\Config\SOFTWARE    Disabled
0xa303124b0000  \Device\HarddiskVolume1\Boot\BCD        Disabled
0xa3031282b000  \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT        Disabled
0xa30312a47000  \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  Disabled
0xa30312a3e000  \SystemRoot\System32\Config\BBI Disabled
0xa30313e2c000  \??\C:\Windows\AppCompat\Programs\Amcache.hve   Disabled
0xa30314219000  \??\C:\Users\Denisha\ntuser.dat Disabled
0xa30314774000  \??\C:\Users\Denisha\AppData\Local\Microsoft\Windows\UsrClass.dat       Disabled
0xa30316deb000  \SystemRoot\System32\config\DRIVERS     Disabled
0xa30317618000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Search_1.14.2.19041_neutral_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 0xa30314774000 --key AtomicRedTeam
Using this command find the detail about
Atomic RedTeam key value(any key enter).
13:33
22-07-2023

Super Timeline Analysis

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

1. Prepare Tools

Volatility3
Plaso Log2Timeline
QEMU

2. Prepare Evidence

Disk image(RAW!)
Memory image

3. Run Tools

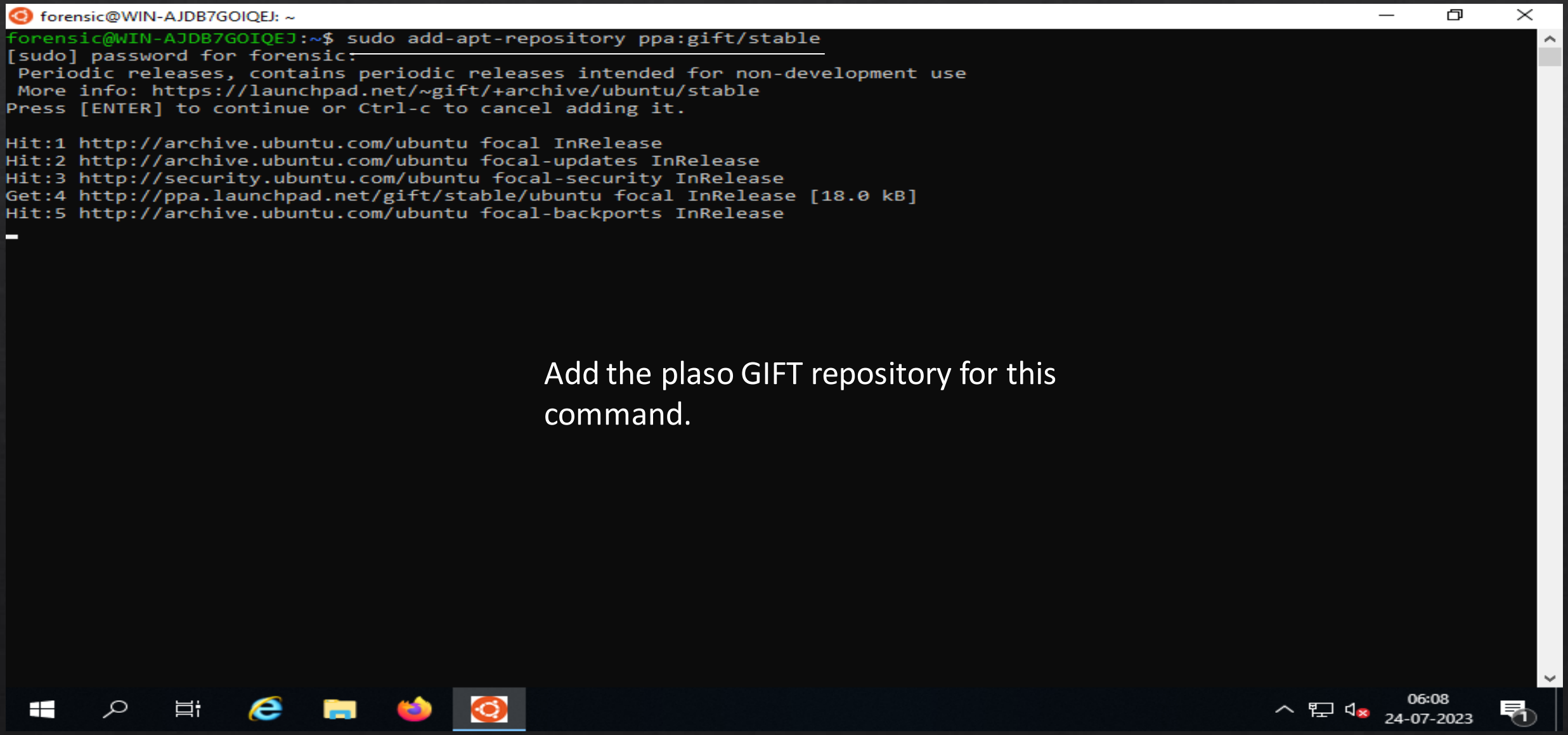
Memory-generate bodyfile
Disk-generate plaso file
Merge files
Generate super timeline with psort

4. Timeline Analysis

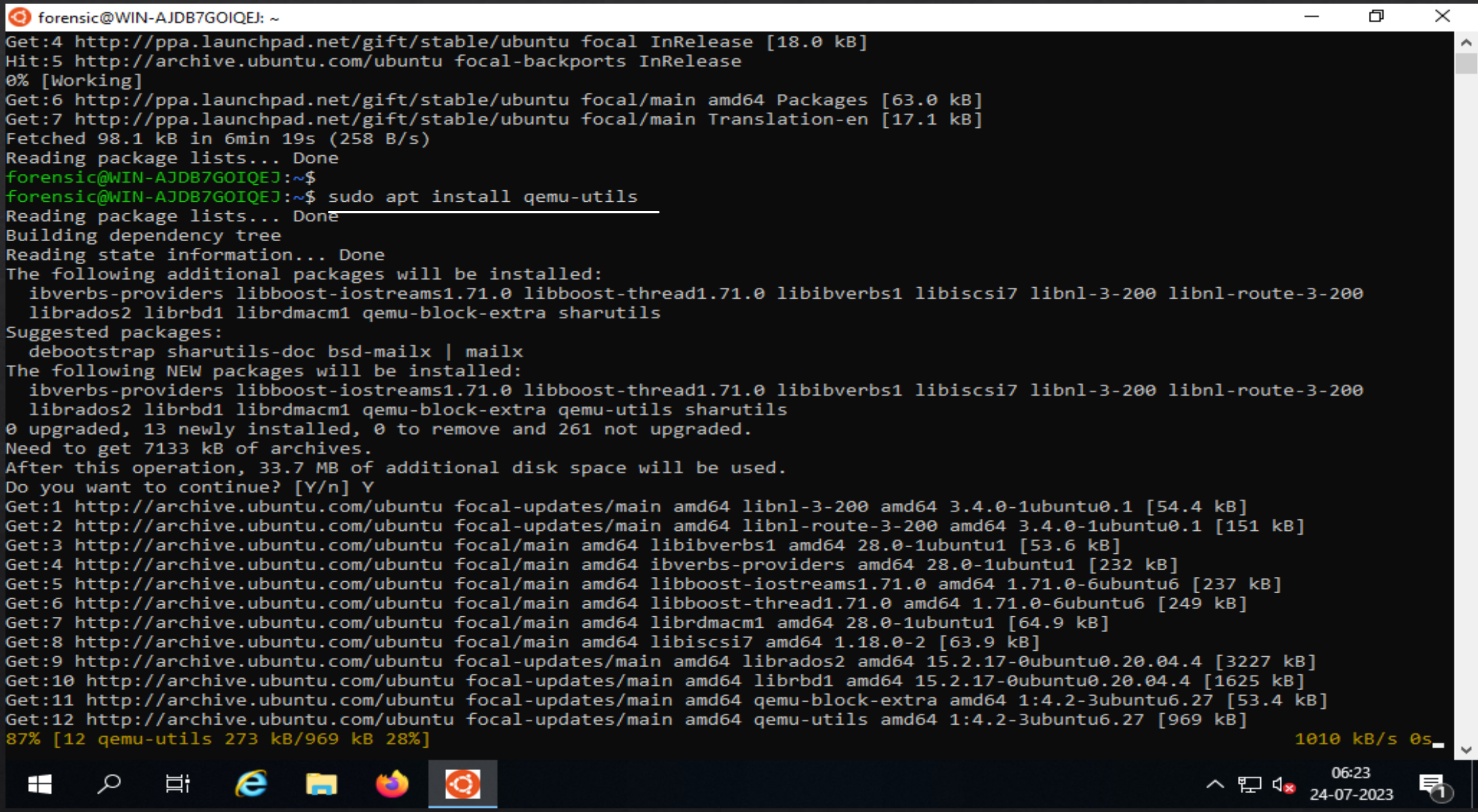
EZ Timeline Explorer

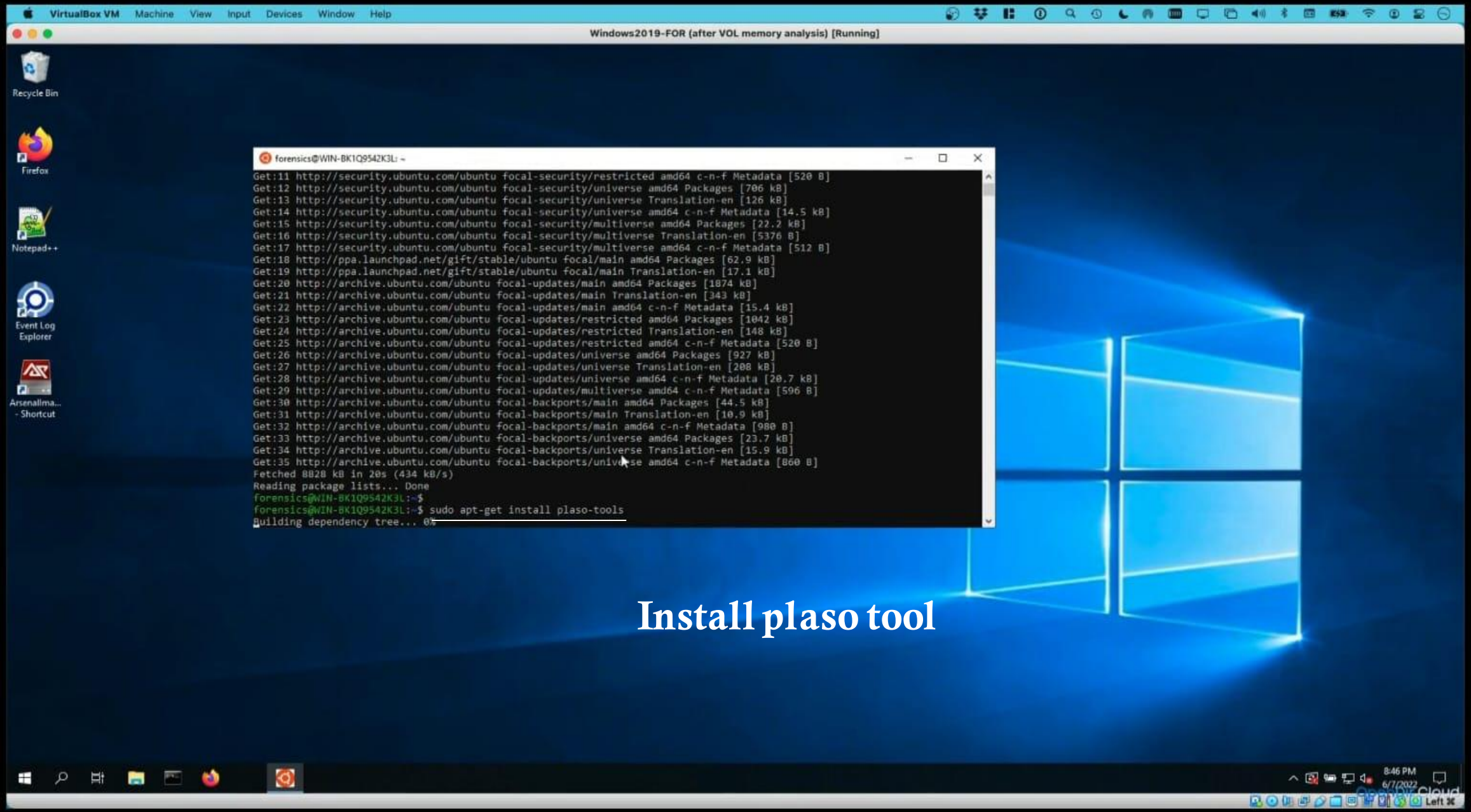
Prepare tools and Converting the disk image with QEMU

Use the link for install the Tools

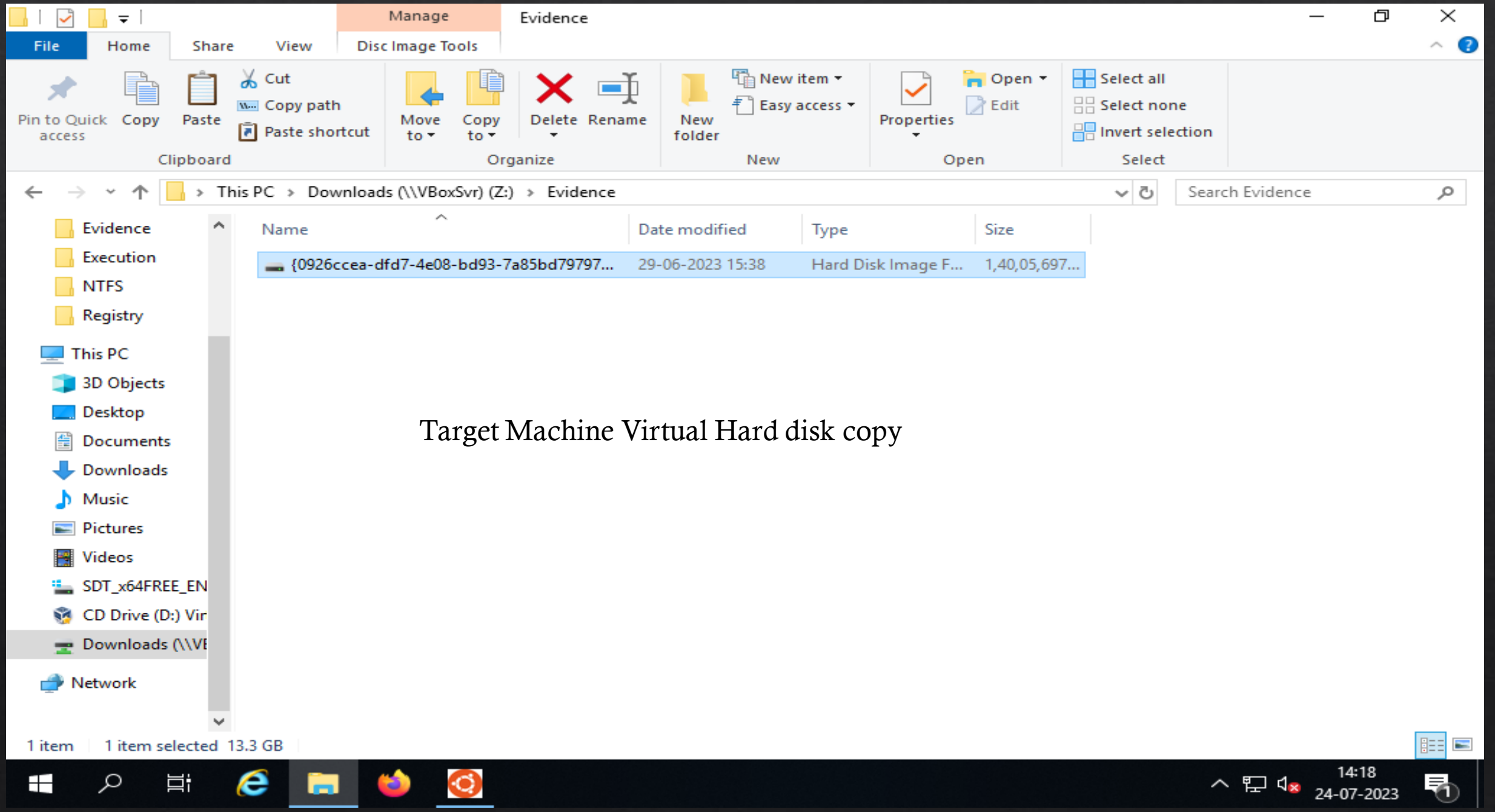


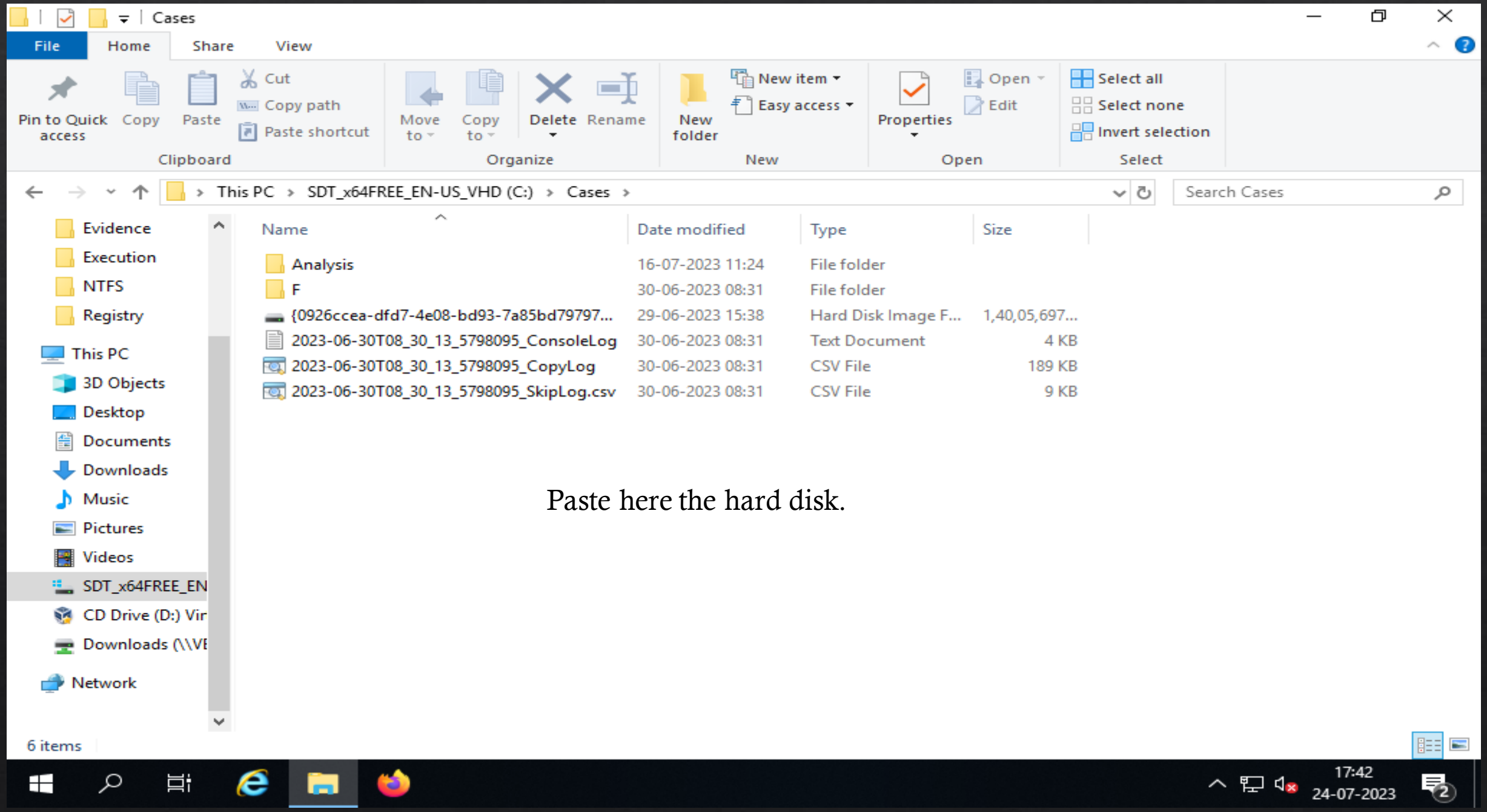
Add the plaso GIFT repository for this command.

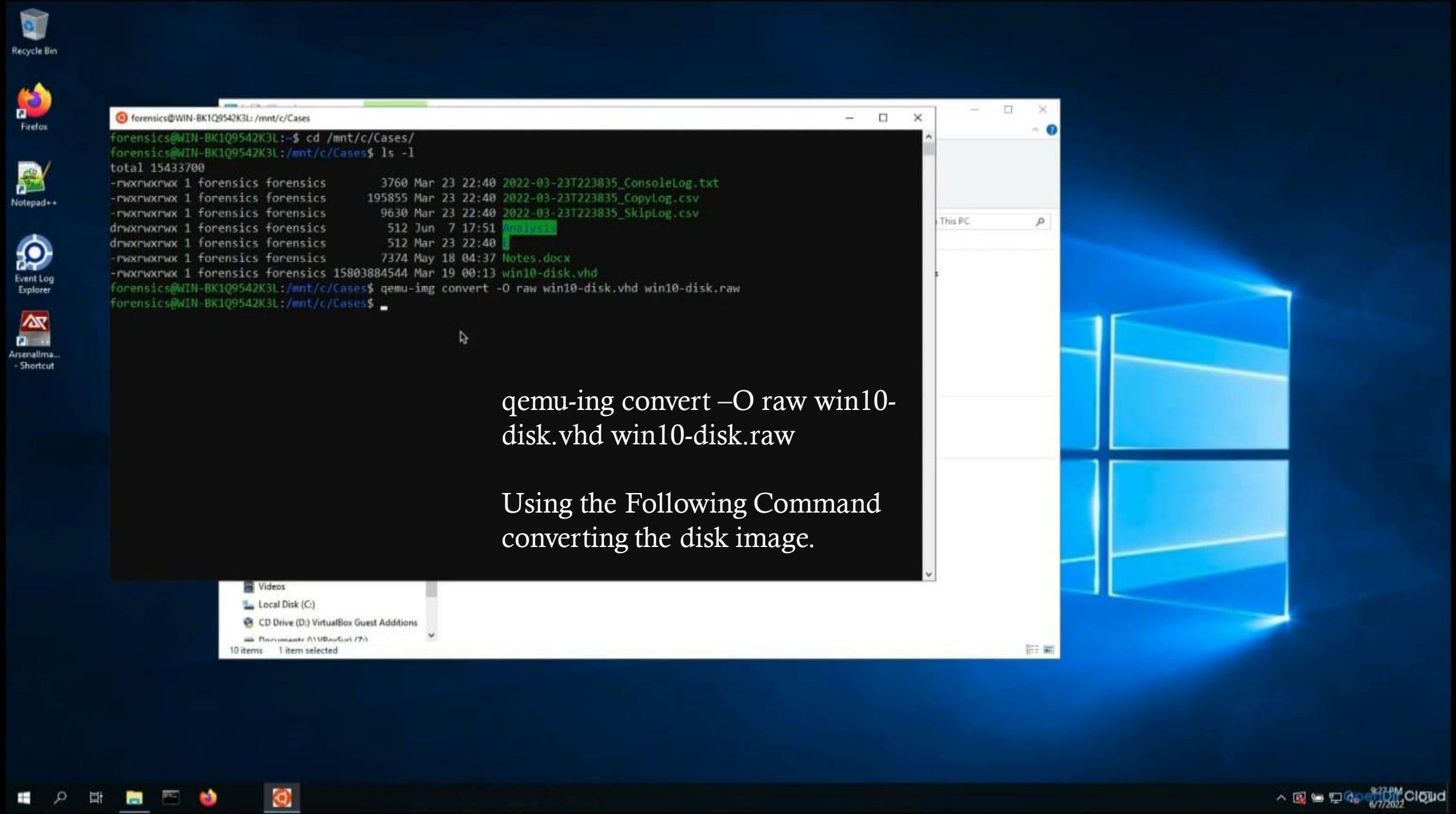

forensic@WIN-AJDB7GOIQEJ: ~
Get:4 http://ppa.launchpad.net/gift/stable/ubuntu focal InRelease [18.0 kB]
Hit:5 http://archive.ubuntu.com/ubuntu focal-backports InRelease
0% [Working]
Get:6 http://ppa.launchpad.net/gift/stable/ubuntu focal/main amd64 Packages [63.0 kB]
Get:7 http://ppa.launchpad.net/gift/stable/ubuntu focal/main Translation-en [17.1 kB]
Fetched 98.1 kB in 6min 19s (258 B/s)
Reading package lists... Done
forensic@WIN-AJDB7GOIQEJ:~$
forensic@WIN-AJDB7GOIQEJ:~$ sudo apt install qemu-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
ibverbs-providers libboost-iostreams1.71.0 libboost-thread1.71.0 libibverbs1 libiscsi7 libnl-3-200 libnl-route-3-200
librados2 librbd1 librdmacm1 qemu-block-extra sharutils
Suggested packages:
debootstrap sharutils-doc bsd-mailx | mailx
The following NEW packages will be installed:
ibverbs-providers libboost-iostreams1.71.0 libboost-thread1.71.0 libibverbs1 libiscsi7 libnl-3-200 libnl-route-3-200
librados2 librbd1 librdmacm1 qemu-block-extra qemu-utils sharutils
0 upgraded, 13 newly installed, 0 to remove and 261 not upgraded.
Need to get 7133 kB of archives.
After this operation, 33.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 libnl-3-200 amd64 3.4.0-1ubuntu0.1 [54.4 kB]
Get:2 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 libnl-route-3-200 amd64 3.4.0-1ubuntu0.1 [151 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal/main amd64 libibverbs1 amd64 28.0-1ubuntu1 [53.6 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal/main amd64 ibverbs-providers amd64 28.0-1ubuntu1 [232 kB]
Get:5 http://archive.ubuntu.com/ubuntu focal/main amd64 libboost-iostreams1.71.0 amd64 1.71.0-6ubuntu6 [237 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal/main amd64 libboost-thread1.71.0 amd64 1.71.0-6ubuntu6 [249 kB]
Get:7 http://archive.ubuntu.com/ubuntu focal/main amd64 librdmacm1 amd64 28.0-1ubuntu1 [64.9 kB]
Get:8 http://archive.ubuntu.com/ubuntu focal/main amd64 libiscsi7 amd64 1.18.0-2 [63.9 kB]
Get:9 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 librados2 amd64 15.2.17-0ubuntu0.20.04.4 [3227 kB]
Get:10 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 librbd1 amd64 15.2.17-0ubuntu0.20.04.4 [1625 kB]
Get:11 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 qemu-block-extra amd64 1:4.2-3ubuntu6.27 [53.4 kB]
Get:12 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 qemu-utils amd64 1:4.2-3ubuntu6.27 [969 kB]
87% [12 qemu-utils 273 kB/969 kB 28%] 1010 kB/s 0s
06:23
24-07-2023

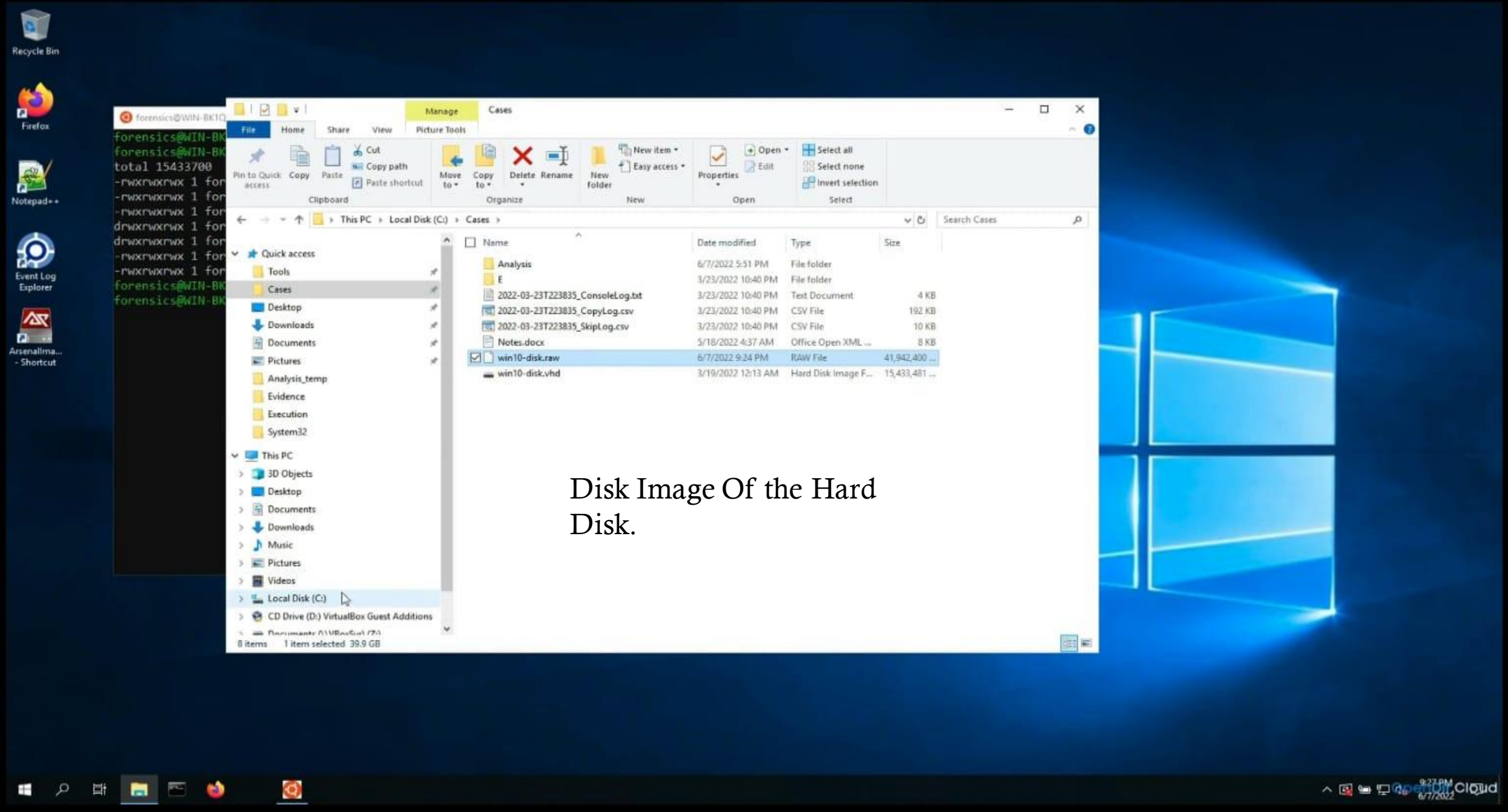


Install plaso tool


Manage
Evidence
File
Home
Share
View
Disc Image Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
Open
Select all
Select none
Invert selection
Select
This PC
Downloads (\\VBoxSvr) (Z:)
Evidence
Search Evidence
Evidence
Execution
NTFS
Registry
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
SDT_x64FREE_EN
CD Drive (D:) Vir
Downloads (\\VE
Network
Name
Date modified
Type
Size
{0926ccea-dfd7-4e08-bd93-7a85bd79797...
29-06-2023 15:38
Hard Disk Image F...
1,40,05,697...
Target Machine Virtual Hard disk copy
1 item
1 item selected 13.3 GB
14:18
24-07-2023

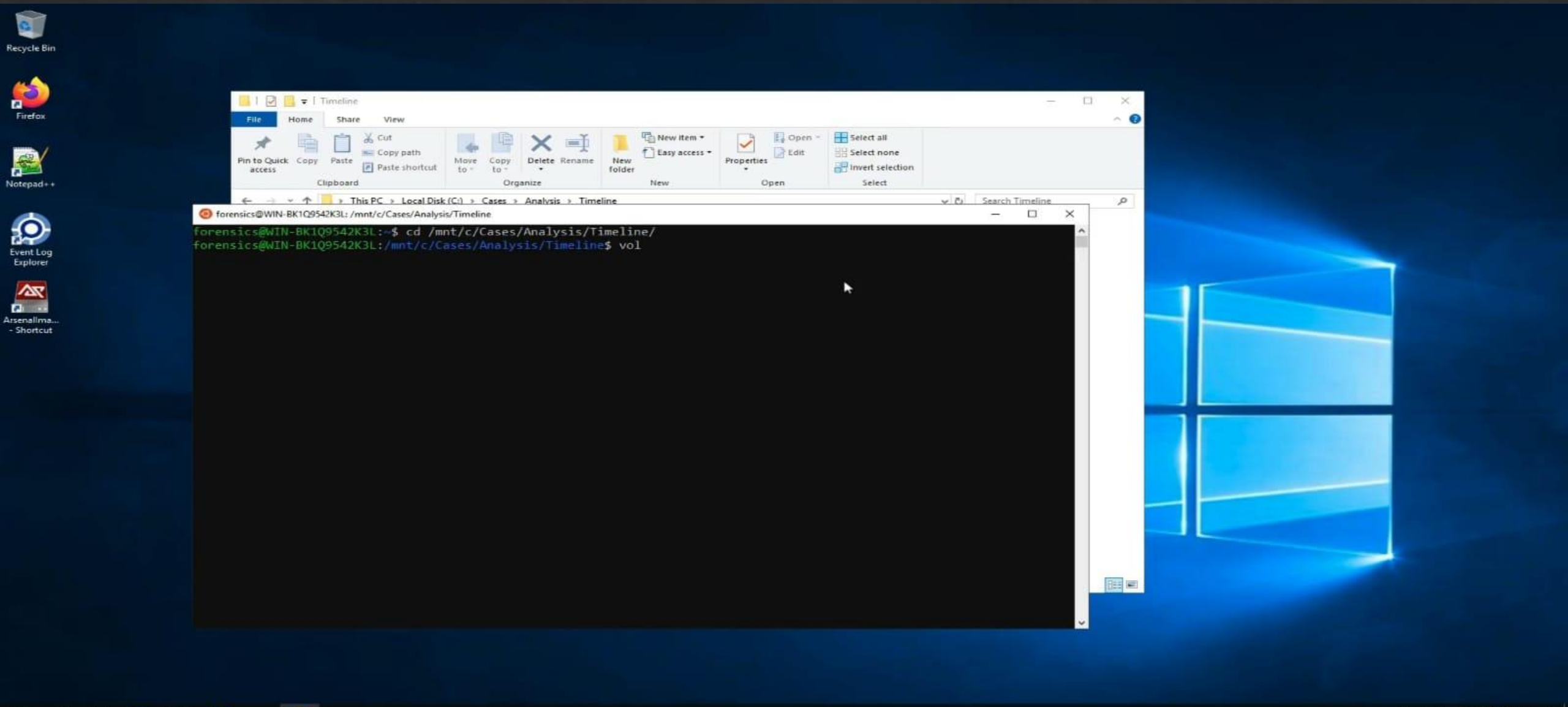

Cases
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New item
Easy access
New folder
New
Properties
Open
Edit
Open
Select all
Select none
Invert selection
Select
This PC
SDT_x64FREE_EN-US_VHD (C:)
Cases
Search Cases
Evidence
Execution
NTFS
Registry
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
SDT_x64FREE_EN
CD Drive (D:) Vir
Downloads (\\VE
Network
Name
Date modified
Type
Size
Analysis
16-07-2023 11:24
File folder
F
30-06-2023 08:31
File folder
{0926ccea-dfd7-4e08-bd93-7a85bd79797...
29-06-2023 15:38
Hard Disk Image F...
1,40,05,697...
2023-06-30T08_30_13_5798095_ConsoleLog
30-06-2023 08:31
Text Document
4 KB
2023-06-30T08_30_13_5798095_CopyLog
30-06-2023 08:31
CSV File
189 KB
2023-06-30T08_30_13_5798095_SkipLog.csv
30-06-2023 08:31
CSV File
9 KB
Paste here the hard disk.
6 items
17:42
24-07-2023

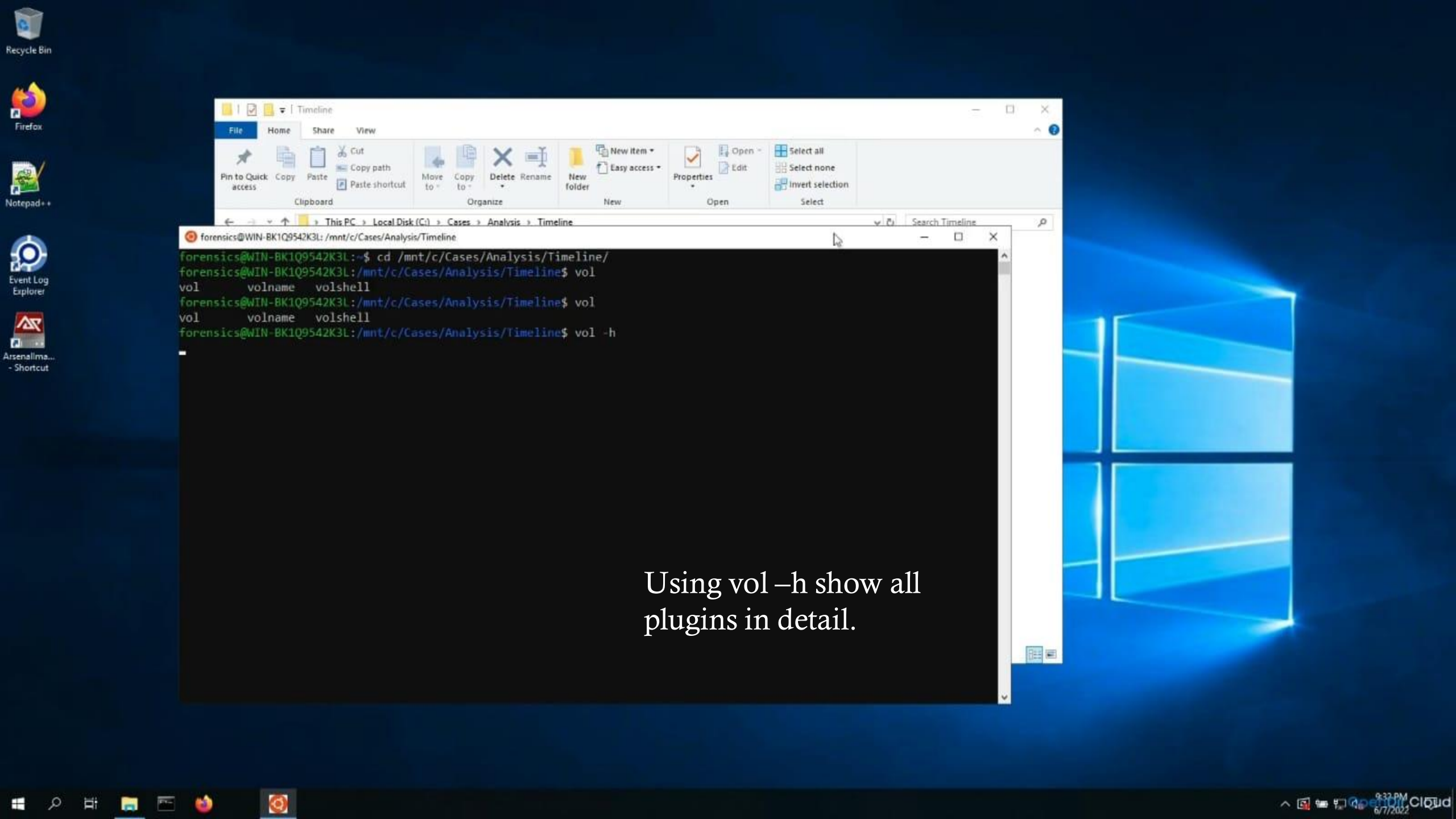

Recycle Bin
Firefox
Notepad++
Event Log Explorer
Arsenalima... - Shortcut
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases
forensics@WIN-BK1Q9542K3L:~$ cd /mnt/c/Cases/
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases$ ls -l
total 15433700
-rwxrwxrwx 1 forensics forensics 3760 Mar 23 22:40 2022-03-23T223835_ConsoleLog.txt
-rwxrwxrwx 1 forensics forensics 195855 Mar 23 22:40 2022-03-23T223835_CopyLog.csv
-rwxrwxrwx 1 forensics forensics 9630 Mar 23 22:40 2022-03-23T223835_SkipLog.csv
drwxrwxrwx 1 forensics forensics 512 Jun 7 17:51 Analysis
drwxrwxrwx 1 forensics forensics 512 Mar 23 22:40 E
-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$
This PC
Videos
Local Disk (C:)
CD Drive (D:) VirtualBox Guest Additions
10 items 1 item selected
qemu-ing convert –O raw win10-disk.vhd win10-disk.raw
Using the Following Command converting the disk image.

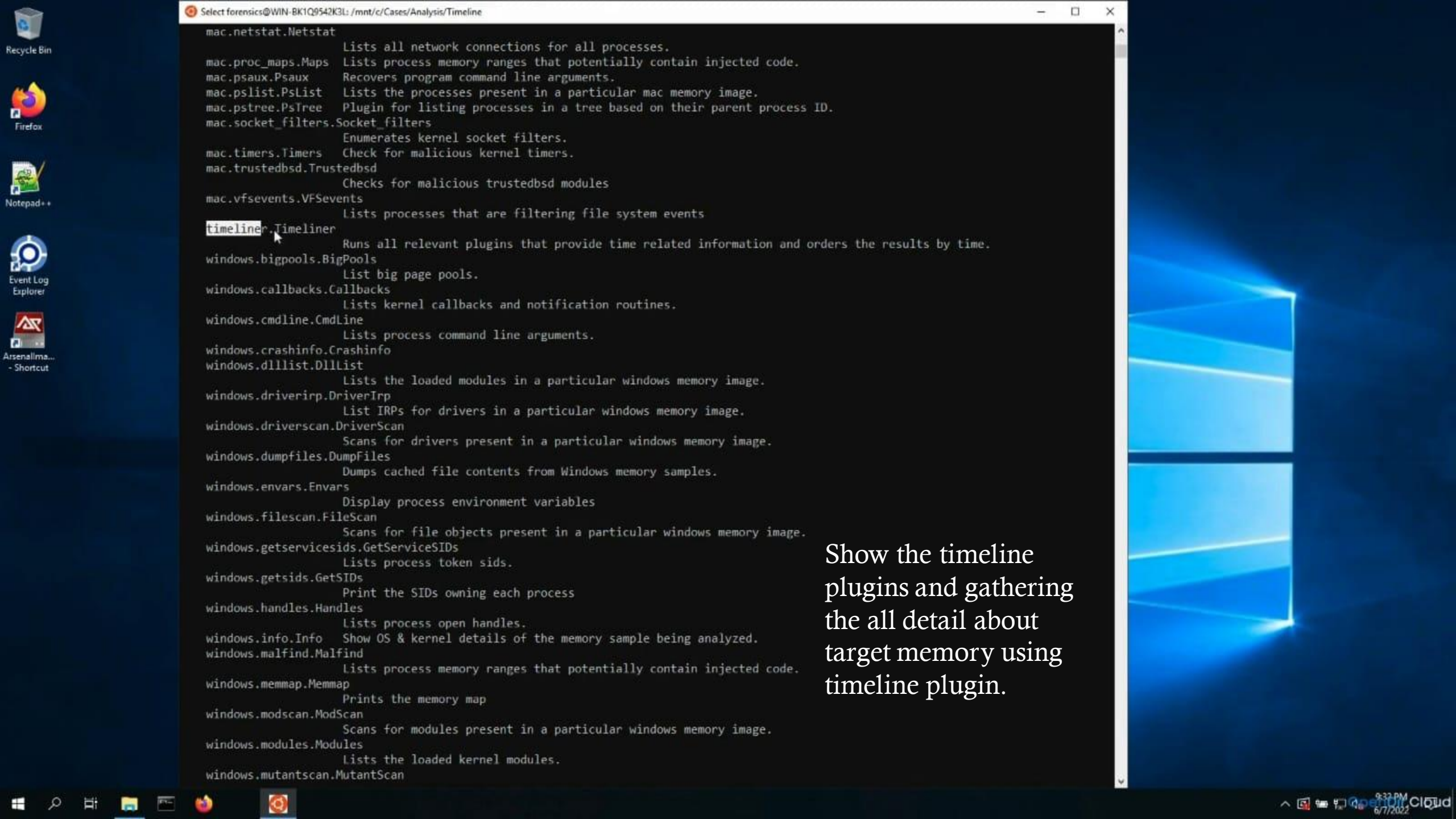

Recycle Bin
Firefox
Notepad++
Event Log Explorer
ArsenalIma... - Shortcut
forensics@WIN-BK1Q
forensics@WIN-BK
forensics@WIN-BK
total 15433700
-rwxrwxrwx 1 for
-rwxrwxrwx 1 for
-rwxrwxrwx 1 for
drwxrwxrwx 1 for
drwxrwxrwx 1 for
-rwxrwxrwx 1 for
-rwxrwxrwx 1 for
forensics@WIN-BK
forensics@WIN-BK
Manage
Cases
File
Home
Share
View
Picture Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
Open
Select all
Select none
Invert selection
Select
This PC
Local Disk (C:)
Cases
Search Cases
Quick access
Tools
Cases
Desktop
Downloads
Documents
Pictures
Analysis_temp
Evidence
Execution
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CD Drive (D:) VirtualBox Guest Additions
Name
Date modified
Type
Size
Analysis
6/7/2022 5:51 PM
File folder
E
3/23/2022 10:40 PM
File folder
2022-03-23T223835_ConsoleLog.txt
3/23/2022 10:40 PM
Text Document
4 KB
2022-03-23T223835_CopyLog.csv
3/23/2022 10:40 PM
CSV File
192 KB
2022-03-23T223835_SkipLog.csv
3/23/2022 10:40 PM
CSV File
10 KB
Notes.docx
5/18/2022 4:37 AM
Office Open XML ...
8 KB
win10-disk.raw
6/7/2022 9:24 PM
RAW File
41,942,400 ...
win10-disk.vhd
3/19/2022 12:13 AM
Hard Disk Image F...
15,433,481 ...
8 items
1 item selected 39.9 GB
Disk Image Of the Hard Disk.

Memory timeline creation with Volatility3

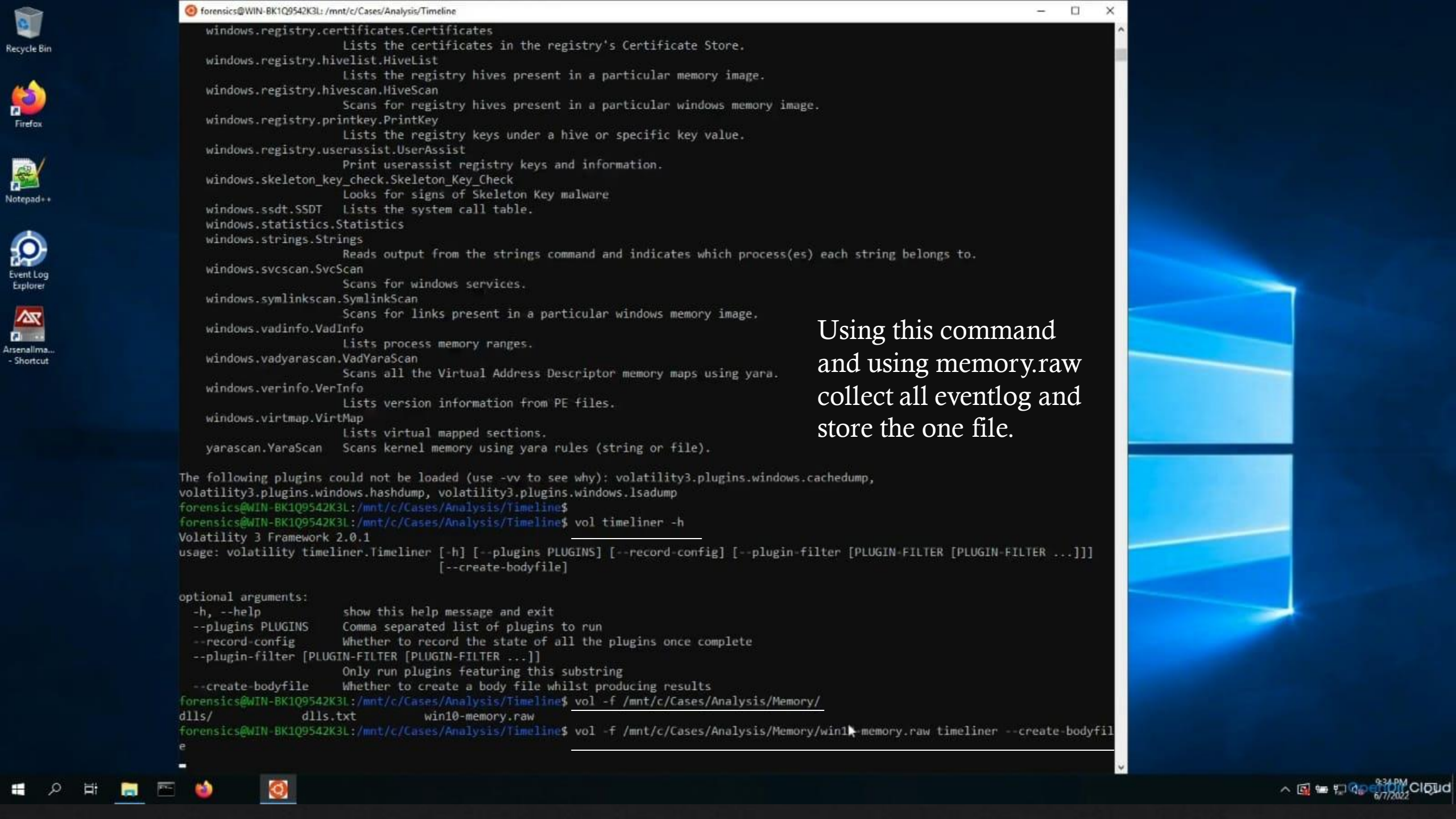
Create a folder Timeline . Go to the folder path in ubuntu linux.

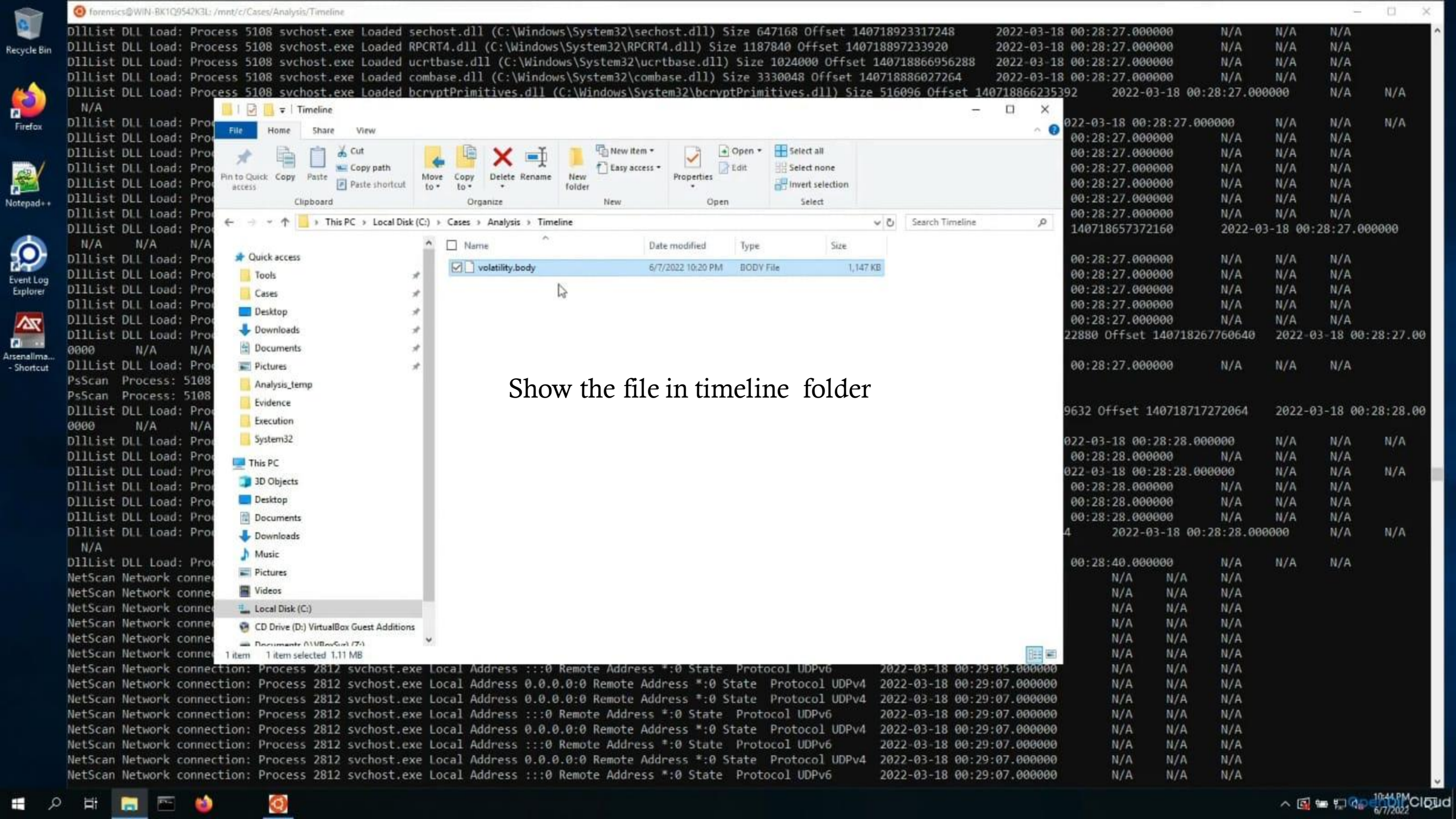


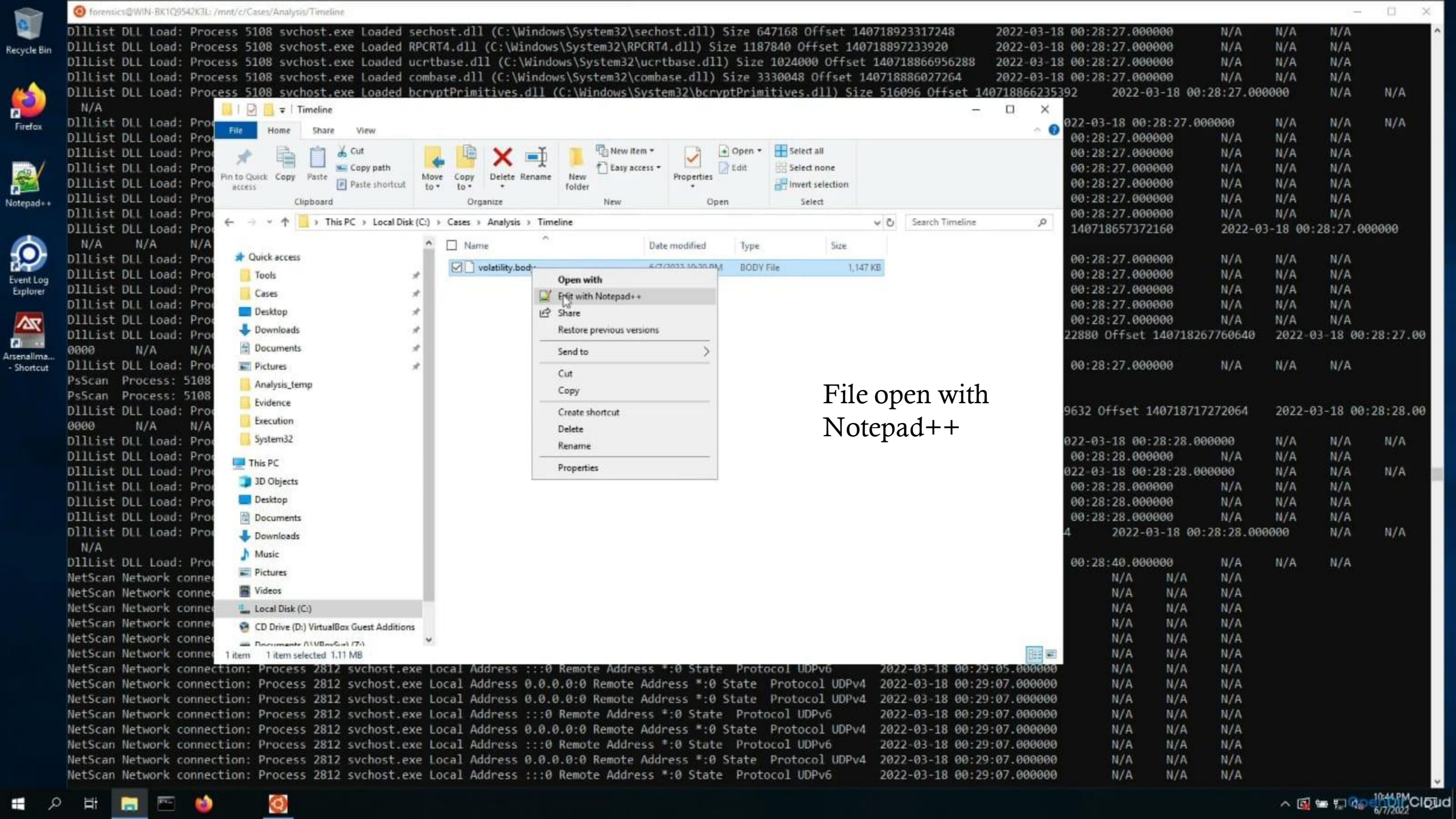

Recycle Bin
Firefox
Notepad++
Event Log Explorer
ArsenalIma... - Shortcut
Timeline
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
Open
Select all
Select none
Invert selection
Select
This PC › Local Disk (C:) › Cases › Analysis › Timeline
Search Timeline
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline
forensics@WIN-BK1Q9542K3L:~$ cd /mnt/c/Cases/Analysis/Timeline/
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ vol
vol volname volshell
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ vol
vol volname volshell
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ vol -h
Using vol –h show all plugins in detail.

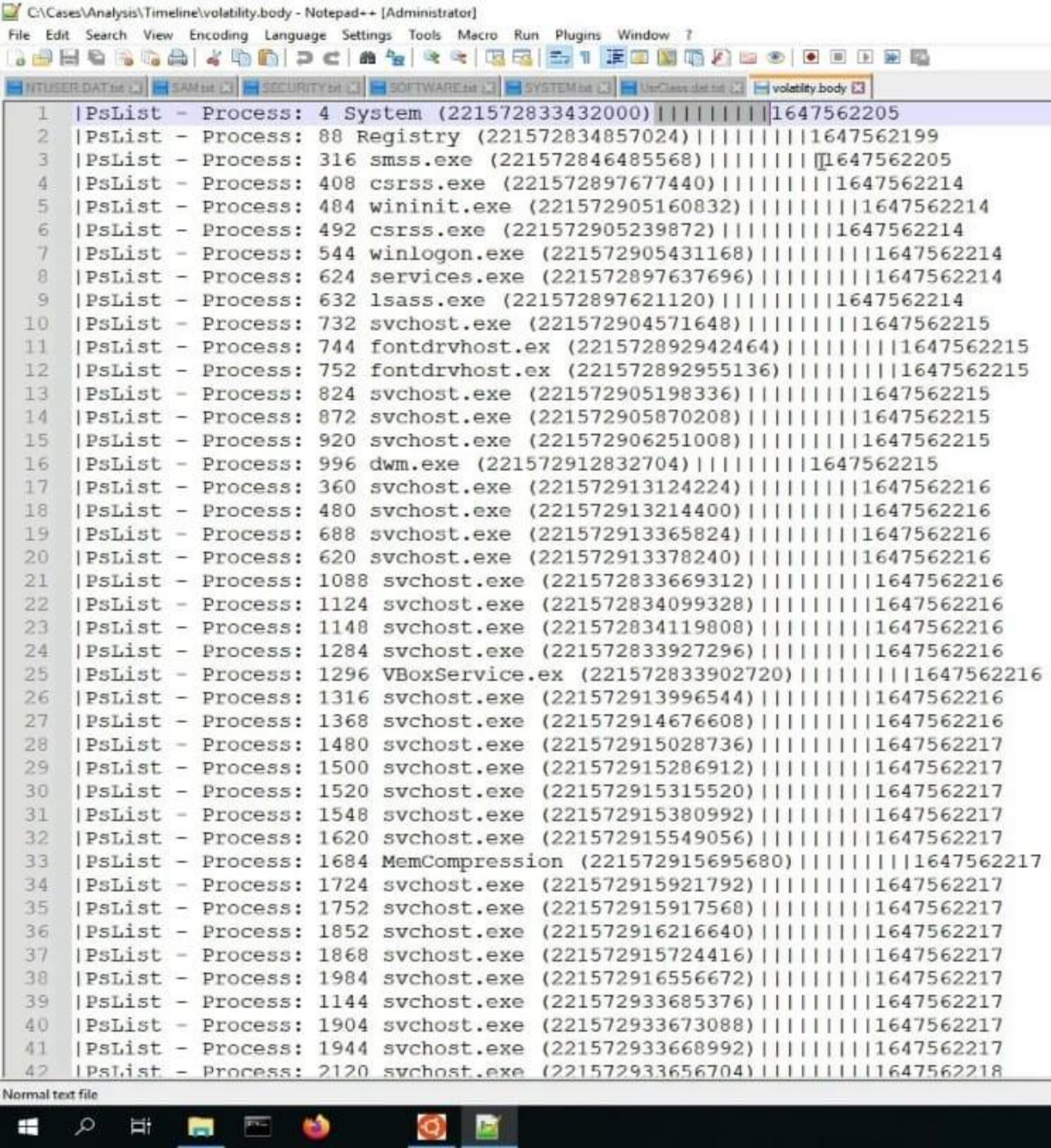


Show the timeline plugins and gathering the all detail about target memory using timeline plugin.


forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline
windows.registry.certificates.Certificates
Lists the certificates in the registry's Certificate Store.
windows.registry.hivelist.HiveList
Lists the registry hives present in a particular memory image.
windows.registry.hivescan.HiveScan
Scans for registry hives present in a particular windows memory image.
windows.registry.printkey.PrintKey
Lists the registry keys under a hive or specific key value.
windows.registry.userassist.UserAssist
Print userassist registry keys and information.
windows.skeleton_key_check.Skeleton_Key_Check
Looks for signs of Skeleton Key malware
windows.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$
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/win1
memory.raw timeliner --create-bodyfil
e
Using this command and using memory.raw collect all eventlog and store the one file.

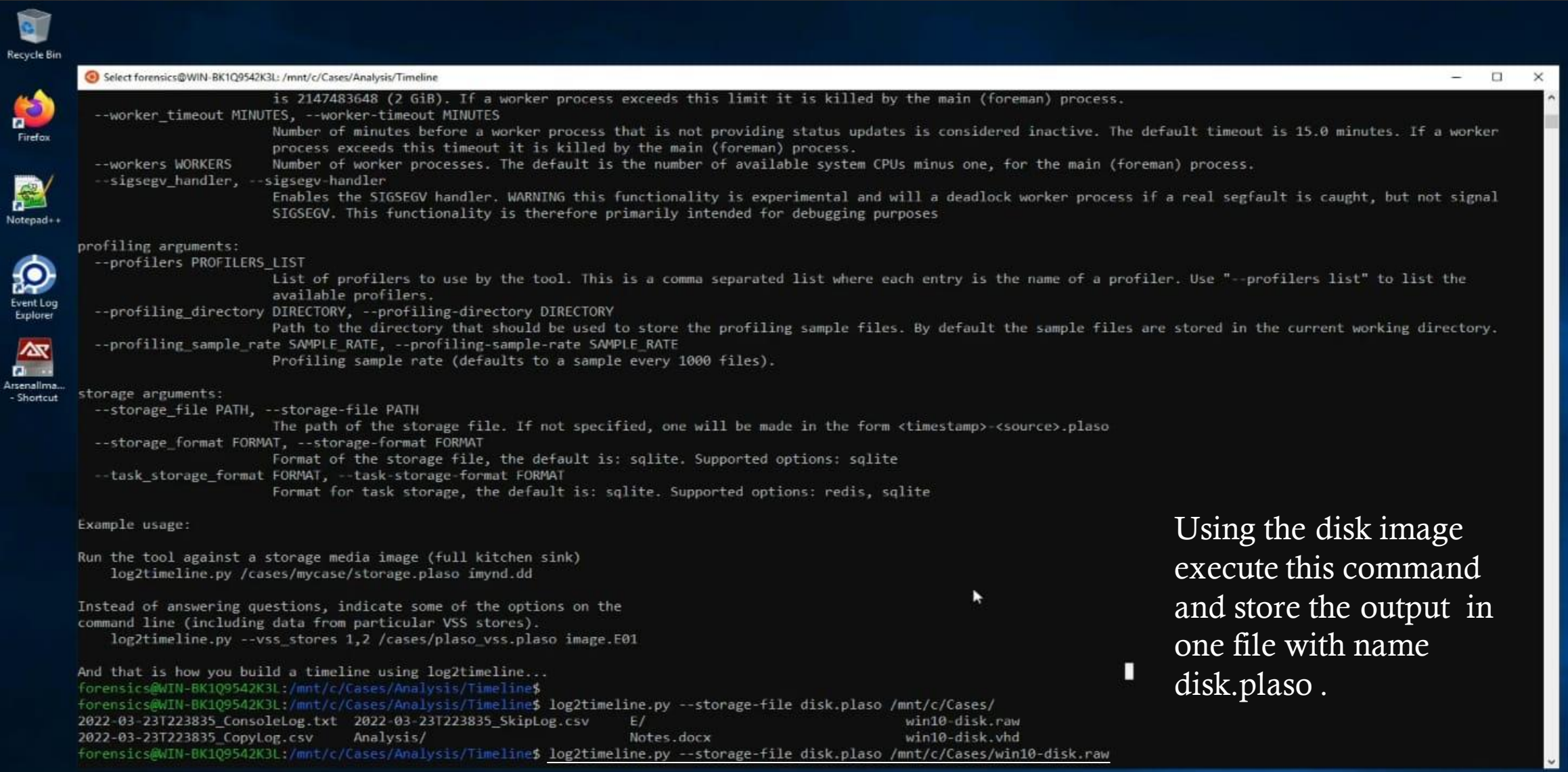

Timeline
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New item
Easy access
New folder
New
Properties
Open
Edit
Open
Select all
Select none
Invert selection
Select
This PC
Local Disk (C:)
Cases
Analysis
Timeline
Search Timeline
Quick access
Tools
Cases
Desktop
Downloads
Documents
Pictures
Analysis_temp
Evidence
Execution
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CD Drive (D:) VirtualBox Guest Additions
Name
Date modified
Type
Size
volatility.body
6/7/2022 10:20 PM
BODY File
1,147 KB
1 item
1 item selected 1.11 MB
Show the file in timeline folder


Timeline
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New item
Easy access
New folder
New
Properties
Open
Edit
Open
Select all
Select none
Invert selection
Select
This PC
Local Disk (C:)
Cases
Analysis
Timeline
Search Timeline
Quick access
Tools
Cases
Desktop
Downloads
Documents
Pictures
Analysis_temp
Evidence
Execution
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CD Drive (D:) VirtualBox Guest Additions
Name
Date modified
Type
Size
volatility.bod
BODY File
1,147 KB
Open with
Edit with Notepad++
Share
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
1 item
1 item selected 1.11 MB
File open with Notepad++

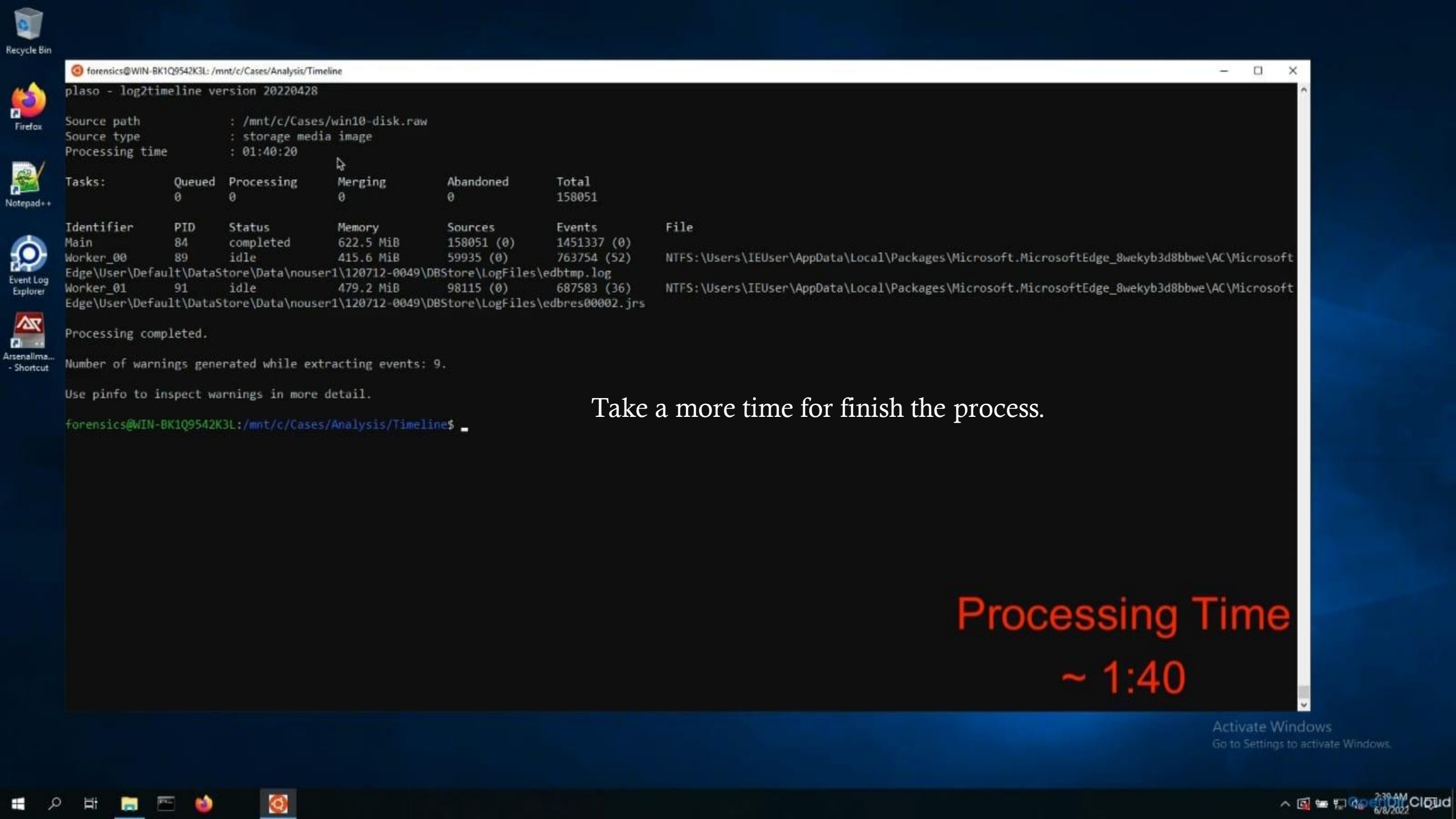


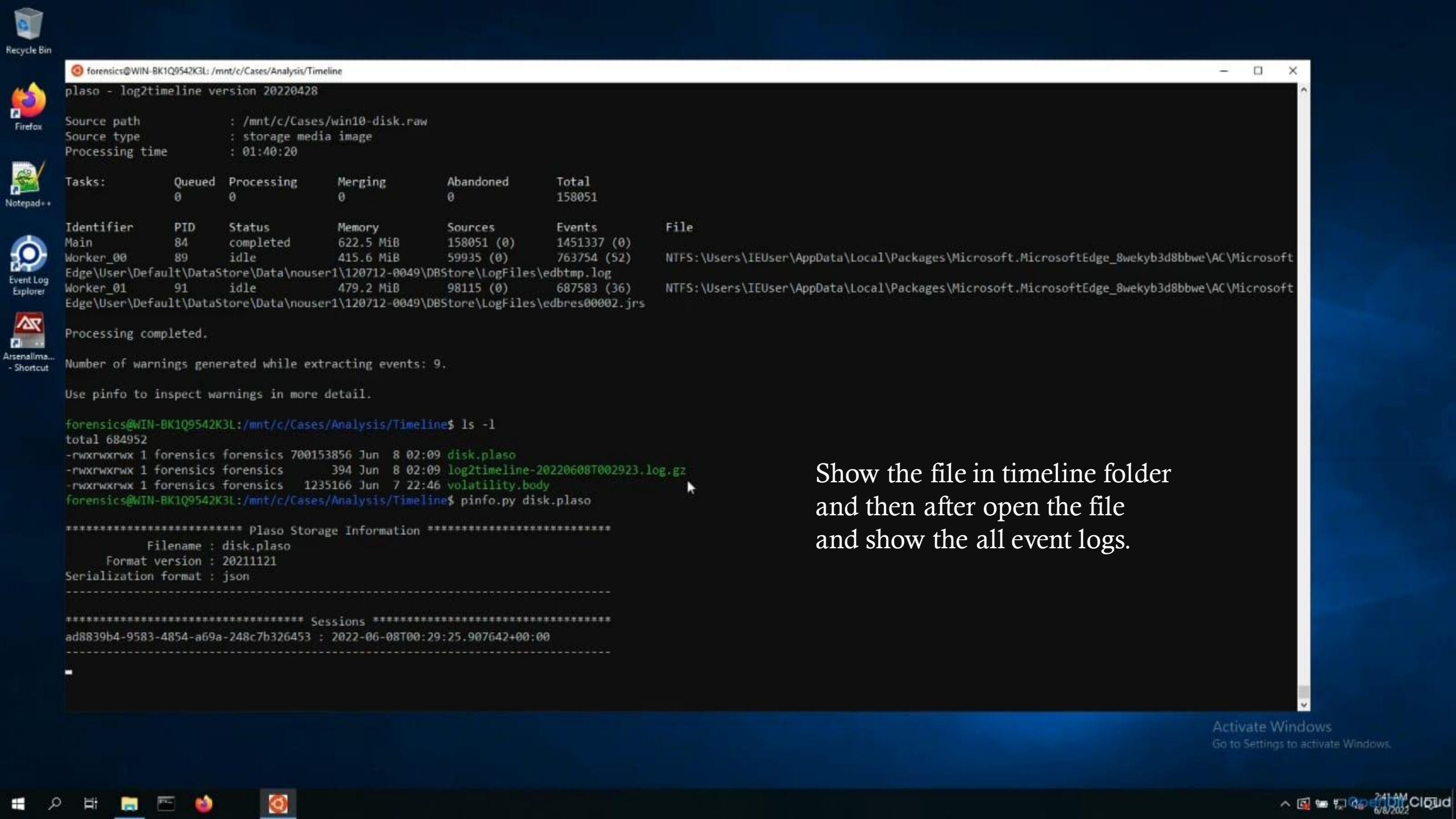
Show the All Events.

Creating a Timeline of the disk image with Plaso tools

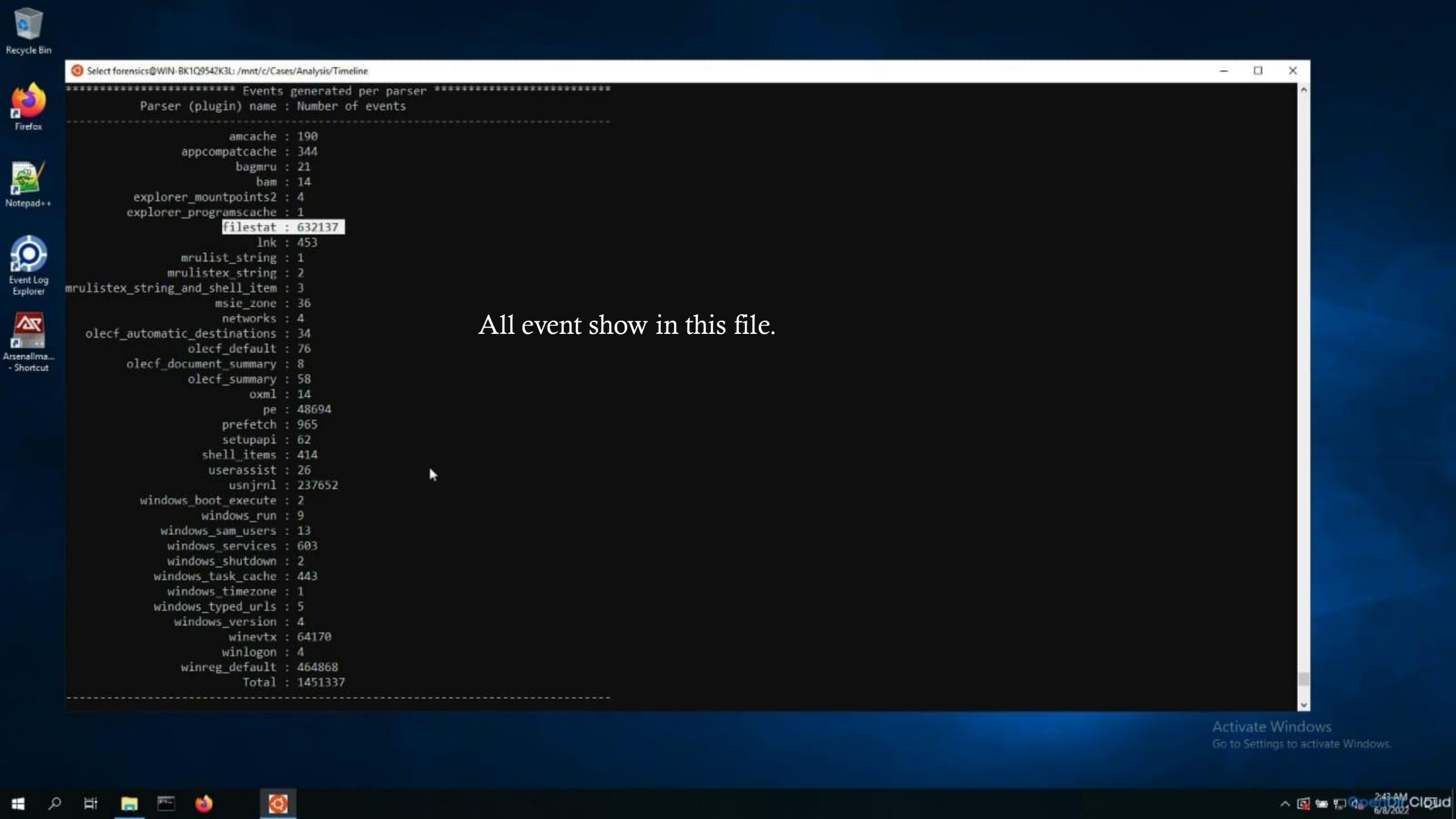


Using the disk image execute this command and store the output in one file with name disk.plaso .


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\MicrosoftEdge\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\MicrosoftEdge\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
Recycle Bin
Firefox
Notepad++
Event Log Explorer
Arsenalima... - Shortcut
Activate Windows
Go to Settings to activate Windows.



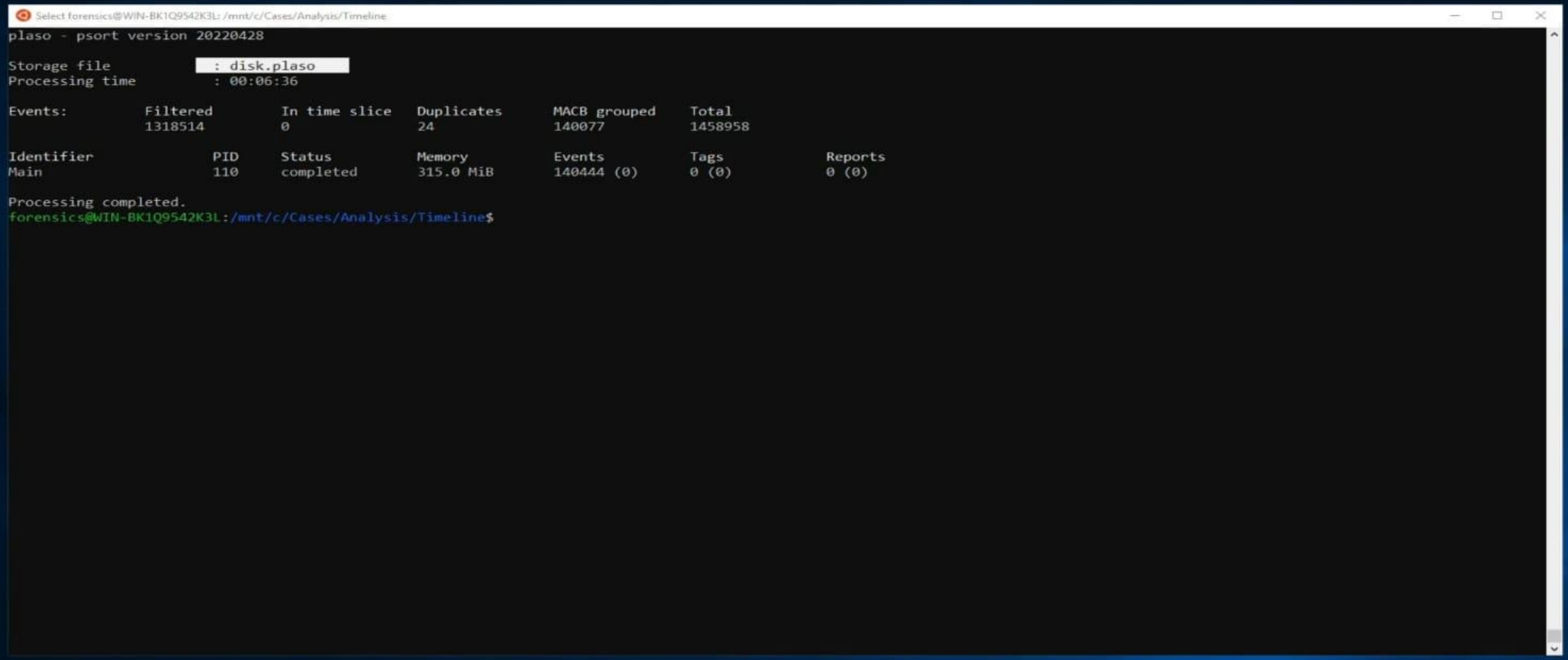
Show the file in timeline folder
and then after open the file
and show the all event logs.

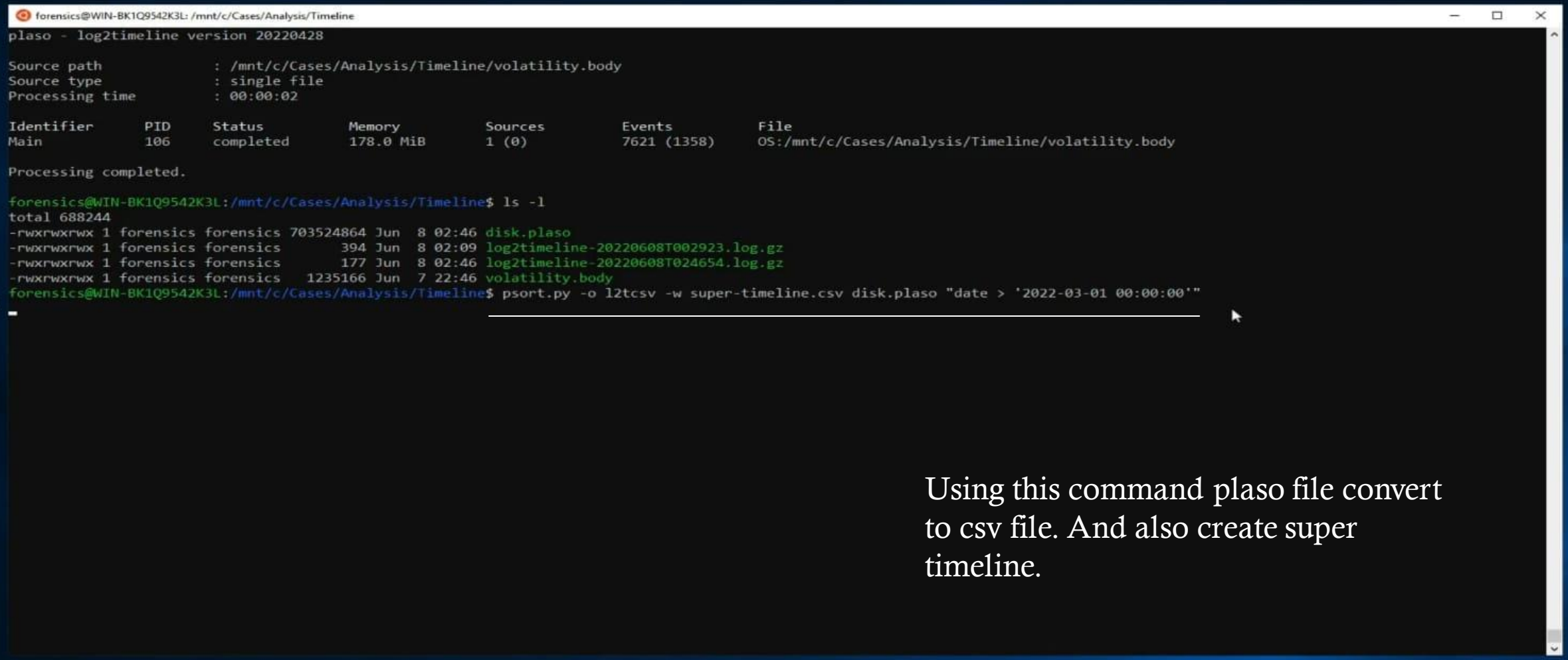

Recycle Bin
Firefox
Notepad++
Event Log Explorer
ArsenalIma... - Shortcut
Select forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline
********** Events generated per parser **********
Parser (plugin) name : Number of events
amcache : 190
appcompatcache : 344
bagmru : 21
bam : 14
explorer_mountpoints2 : 4
explorer_programscache : 1
filestat : 632137
lnk : 453
mrulist_string : 1
mrulistex_string : 2
mrulistex_string_and_shell_item : 3
msie_zone : 36
networks : 4
olecf_automatic_destinations : 34
olecf_default : 76
olecf_document_summary : 8
olecf_summary : 58
oxml : 14
pe : 48694
prefetch : 965
setupapi : 62
shell_items : 414
userassist : 26
usnjrnl : 237652
windows_boot_execute : 2
windows_run : 9
windows_sam_users : 13
windows_services : 603
windows_shutdown : 2
windows_task_cache : 443
windows_timezone : 1
windows_typed_urls : 5
windows_version : 4
winevtx : 64170
winlogon : 4
winreg_default : 464868
Total : 1451337
All event show in this file.
Activate Windows
Go to Settings to activate Windows.

Generating a Super Timeline with plaso tool

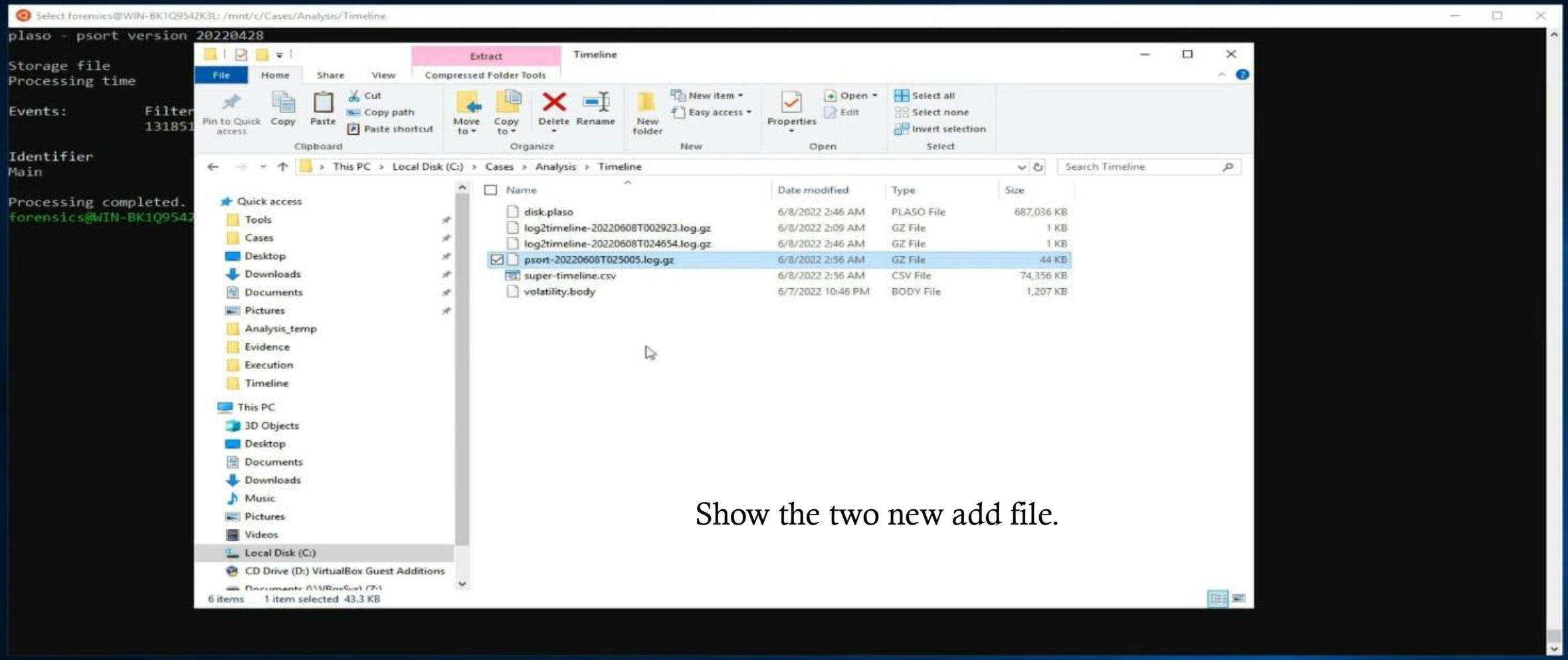
```
forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline
               83 : type: OS, location: /mnt/c/Cases/win10-disk.raw
                  : type: RAW
                  : type: TSK_PARTITION, location: /p1, part index: 2, start
                    offset: 0x00100000
                  : type: NTFS, location:
                    \Windows\System32\winevt\Logs\Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx,
                    MFT attribute: 2, MFT entry: 81143
               78 : type: OS, location: /mnt/c/Cases/win10-disk.raw
                  : type: RAW
                  : type: TSK_PARTITION, location: /p1, part index: 2, start
                    offset: 0x00100000
                  : type: NTFS, location:
                    \Windows\System32\winevt\Logs\Microsoft-Windows-WMI-Activity%4Operational.evtx,
                    MFT attribute: 2, MFT entry: 82820
               76 : type: OS, location: /mnt/c/Cases/win10-disk.raw
                  : type: RAW
                  : type: TSK_PARTITION, location: /p1, part index: 2, start
                    offset: 0x00100000
                  : type: NTFS, location:
                    \Windows\System32\winevt\Logs\Microsoft-Windows-PushNotification-Platform%4Operational.evtx,
                    MFT attribute: 2, MFT entry: 82965
               52 : type: OS, location: /mnt/c/Cases/win10-disk.raw
                  : type: RAW
                  : type: TSK_PARTITION, location: /p1, part index: 2, start
                    offset: 0x00100000
                  : type: NTFS, location:
                    \Windows\System32\winevt\Logs\Microsoft-Windows-Bits-Client%4Operational.evtx,
                    MFT attribute: 2, MFT entry: 82681
---------------------------------------------------------------------------

No analysis reports stored.

forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ ls -l
total 684952
-rwxrwxrwx 1 forensics forensics 700153856 Jun  8 02:09 disk.plaso
-rwxrwxrwx 1 forensics forensics       394 Jun  8 02:09 log2timeline-20220608T002923.log.gz
-rwxrwxrwx 1 forensics forensics   1235166 Jun  7 22:46 volatility.body
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ log2timeline.py --parser=mactime --storage-file=disk.plaso volatility.body
```

Merging timelines with mactime parser using this command.



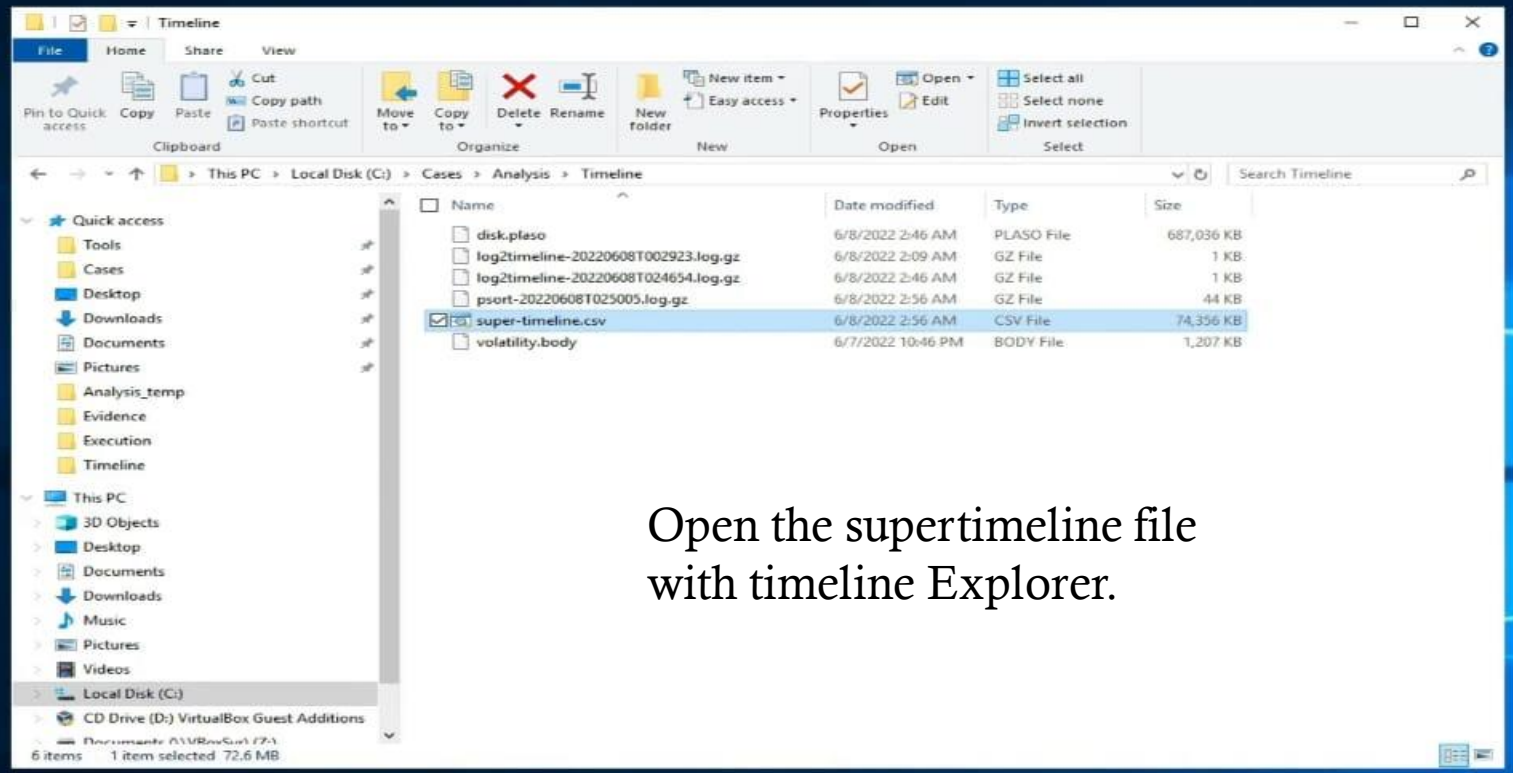


Using this command plaso file convert to csv file. And also create super timeline.

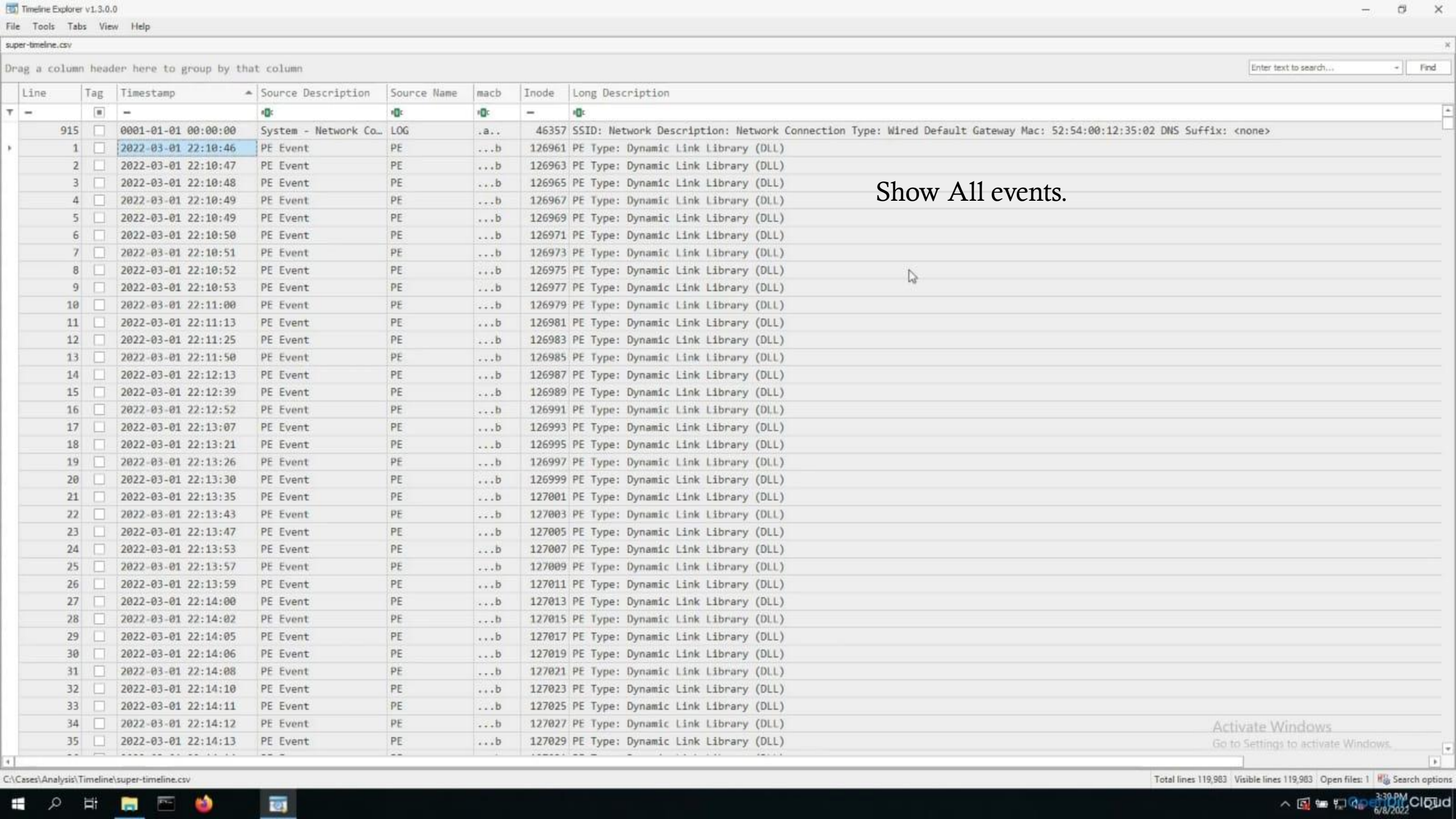

Select forensics@WIN-BK1Q9542K3L: /mnt/c/Cases/Analysis/Timeline
plaso - psort version 20220428
Storage file
Processing time
Events:
Identifier
Main
Processing completed.
Timeline
Extract
File
Home
Share
View
Compressed Folder Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
Select all
Select none
Invert selection
Select
This PC › Local Disk (C:) › Cases › Analysis › Timeline
Search Timeline
Quick access
Tools
Cases
Desktop
Downloads
Documents
Pictures
Analysis_temp
Evidence
Execution
Timeline
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CD Drive (D:) VirtualBox Guest Additions
Name
Date modified
Type
Size
disk.plaso 6/8/2022 2:46 AM PLASO File 687,036 KB
log2timeline-20220608T002923.log.gz 6/8/2022 2:09 AM GZ File 1 KB
log2timeline-20220608T024654.log.gz 6/8/2022 2:46 AM GZ File 1 KB
psort-20220608T025005.log.gz 6/8/2022 2:56 AM GZ File 44 KB
super-timeline.csv 6/8/2022 2:56 AM CSV File 74,356 KB
volatility.body 6/7/2022 10:46 PM BODY File 1,207 KB
6 items
1 item selected 43.3 KB
Show the two new add file.
Activate Windows
Go to Settings to activate Windows.

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.


Timeline Explorer v1.3.0.0
File Tools Tabs View Help
super-timeline.csv
Drag a column header here to group by that column
Enter text to search...
Find
Line | Tag | Timestamp | Source Description | Source Name | macb | Inode | Long Description
915 0001-01-01 00:00:00 System - Network Co… LOG .a.. 46357 SSID: Network Description: Network Connection Type: Wired Default Gateway Mac: 52:54:00:12:35:02 DNS Suffix: <none>
1 2022-03-01 22:10:46 PE Event PE ...b 126961 PE Type: Dynamic Link Library (DLL)
2 2022-03-01 22:10:47 PE Event PE ...b 126963 PE Type: Dynamic Link Library (DLL)
3 2022-03-01 22:10:48 PE Event PE ...b 126965 PE Type: Dynamic Link Library (DLL)
4 2022-03-01 22:10:49 PE Event PE ...b 126967 PE Type: Dynamic Link Library (DLL)
5 2022-03-01 22:10:49 PE Event PE ...b 126969 PE Type: Dynamic Link Library (DLL)
6 2022-03-01 22:10:50 PE Event PE ...b 126971 PE Type: Dynamic Link Library (DLL)
7 2022-03-01 22:10:51 PE Event PE ...b 126973 PE Type: Dynamic Link Library (DLL)
8 2022-03-01 22:10:52 PE Event PE ...b 126975 PE Type: Dynamic Link Library (DLL)
9 2022-03-01 22:10:53 PE Event PE ...b 126977 PE Type: Dynamic Link Library (DLL)
10 2022-03-01 22:11:00 PE Event PE ...b 126979 PE Type: Dynamic Link Library (DLL)
11 2022-03-01 22:11:13 PE Event PE ...b 126981 PE Type: Dynamic Link Library (DLL)
12 2022-03-01 22:11:25 PE Event PE ...b 126983 PE Type: Dynamic Link Library (DLL)
13 2022-03-01 22:11:50 PE Event PE ...b 126985 PE Type: Dynamic Link Library (DLL)
14 2022-03-01 22:12:13 PE Event PE ...b 126987 PE Type: Dynamic Link Library (DLL)
15 2022-03-01 22:12:39 PE Event PE ...b 126989 PE Type: Dynamic Link Library (DLL)
16 2022-03-01 22:12:52 PE Event PE ...b 126991 PE Type: Dynamic Link Library (DLL)
17 2022-03-01 22:13:07 PE Event PE ...b 126993 PE Type: Dynamic Link Library (DLL)
18 2022-03-01 22:13:21 PE Event PE ...b 126995 PE Type: Dynamic Link Library (DLL)
19 2022-03-01 22:13:26 PE Event PE ...b 126997 PE Type: Dynamic Link Library (DLL)
20 2022-03-01 22:13:30 PE Event PE ...b 126999 PE Type: Dynamic Link Library (DLL)
21 2022-03-01 22:13:35 PE Event PE ...b 127001 PE Type: Dynamic Link Library (DLL)
22 2022-03-01 22:13:43 PE Event PE ...b 127003 PE Type: Dynamic Link Library (DLL)
23 2022-03-01 22:13:47 PE Event PE ...b 127005 PE Type: Dynamic Link Library (DLL)
24 2022-03-01 22:13:53 PE Event PE ...b 127007 PE Type: Dynamic Link Library (DLL)
25 2022-03-01 22:13:57 PE Event PE ...b 127009 PE Type: Dynamic Link Library (DLL)
26 2022-03-01 22:13:59 PE Event PE ...b 127011 PE Type: Dynamic Link Library (DLL)
27 2022-03-01 22:14:00 PE Event PE ...b 127013 PE Type: Dynamic Link Library (DLL)
28 2022-03-01 22:14:02 PE Event PE ...b 127015 PE Type: Dynamic Link Library (DLL)
29 2022-03-01 22:14:05 PE Event PE ...b 127017 PE Type: Dynamic Link Library (DLL)
30 2022-03-01 22:14:06 PE Event PE ...b 127019 PE Type: Dynamic Link Library (DLL)
31 2022-03-01 22:14:08 PE Event PE ...b 127021 PE Type: Dynamic Link Library (DLL)
32 2022-03-01 22:14:10 PE Event PE ...b 127023 PE Type: Dynamic Link Library (DLL)
33 2022-03-01 22:14:11 PE Event PE ...b 127025 PE Type: Dynamic Link Library (DLL)
34 2022-03-01 22:14:12 PE Event PE ...b 127027 PE Type: Dynamic Link Library (DLL)
35 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.
C:\Cases\Analysis\Timeline\super-timeline.csv
Total lines 119,983 Visible lines 119,983 Open files: 1 Search options

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

super-timeline.csv

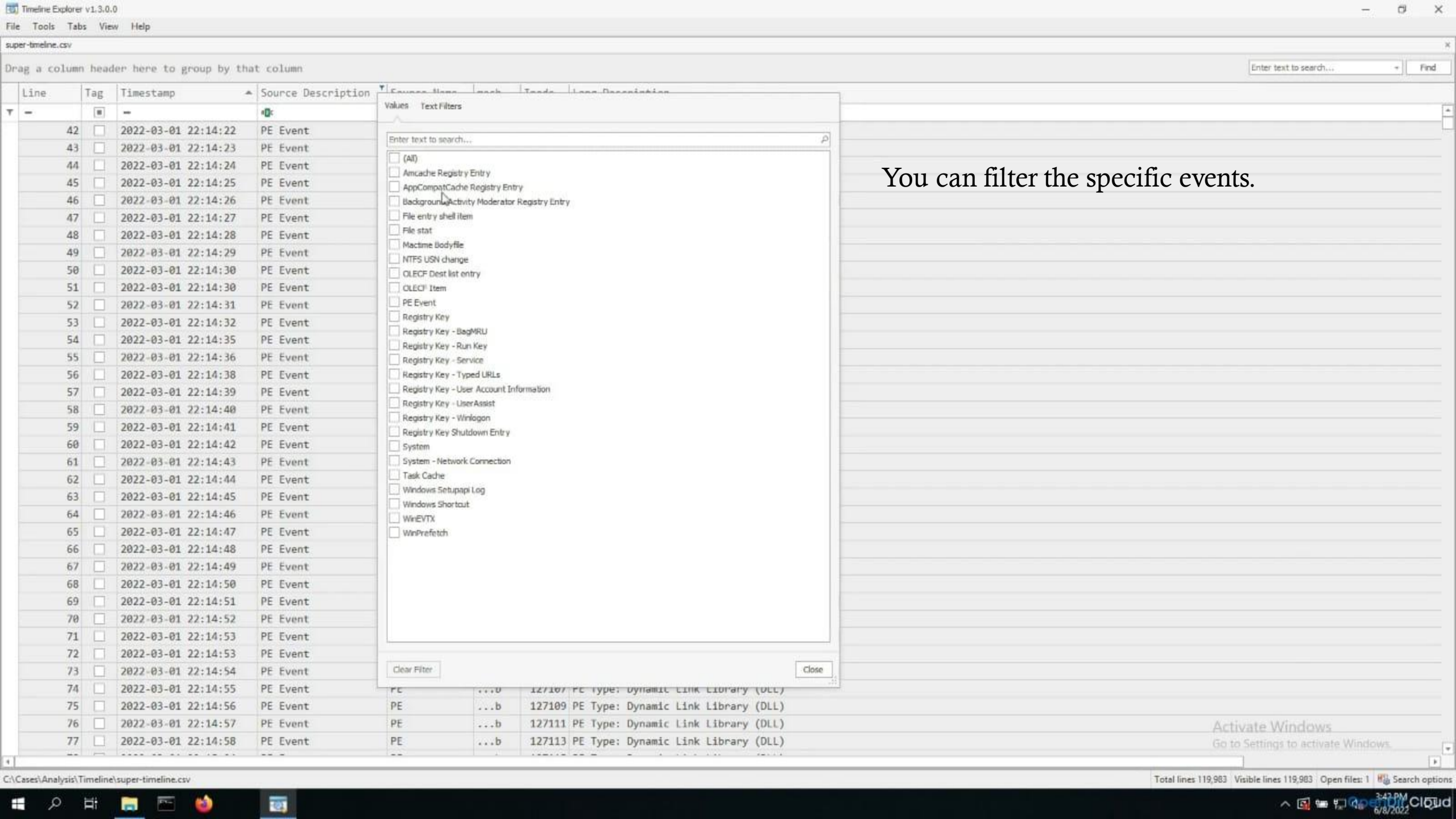
Drag a column header here to group by that column

Enter text to search... Find

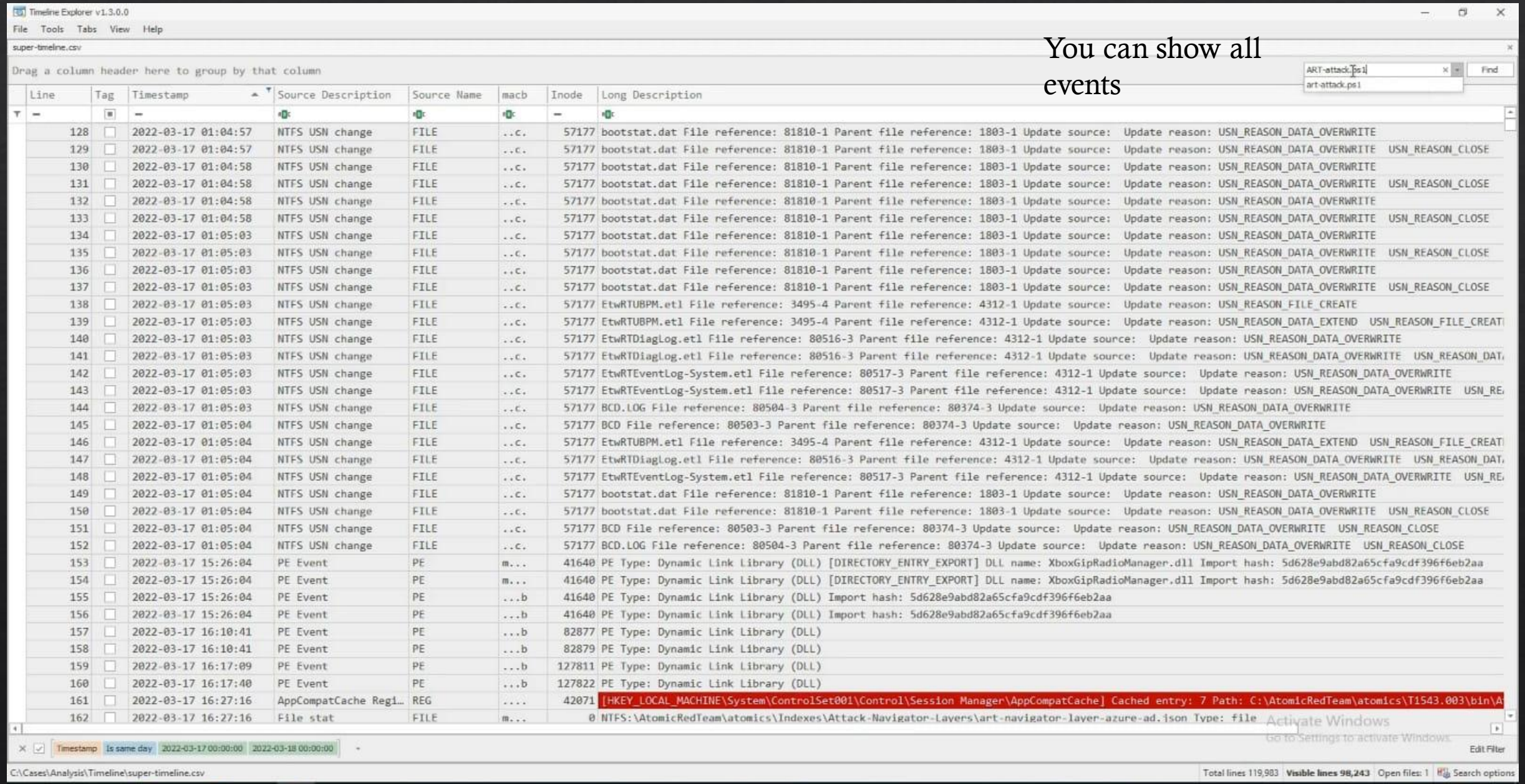
Line	Tag	Timestamp	Source Description	Source Name	macb	Inode	Long Description
66		2022-03-01 22:14:48	PE Event	PE	...b	127091	PE Type: Dynamic Link Library (DLL)
67		2022-03-01 22:14:49	PE Event	PE	...b	127093	PE Type: Dynamic Link Library (DLL)
68		2022-03-01 22:14:50	PE Event	PE	...b	127095	PE Type: 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 22:16:10	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\wpndm\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

C:\Cases\Analysis\Timeline\super-timeline.csv

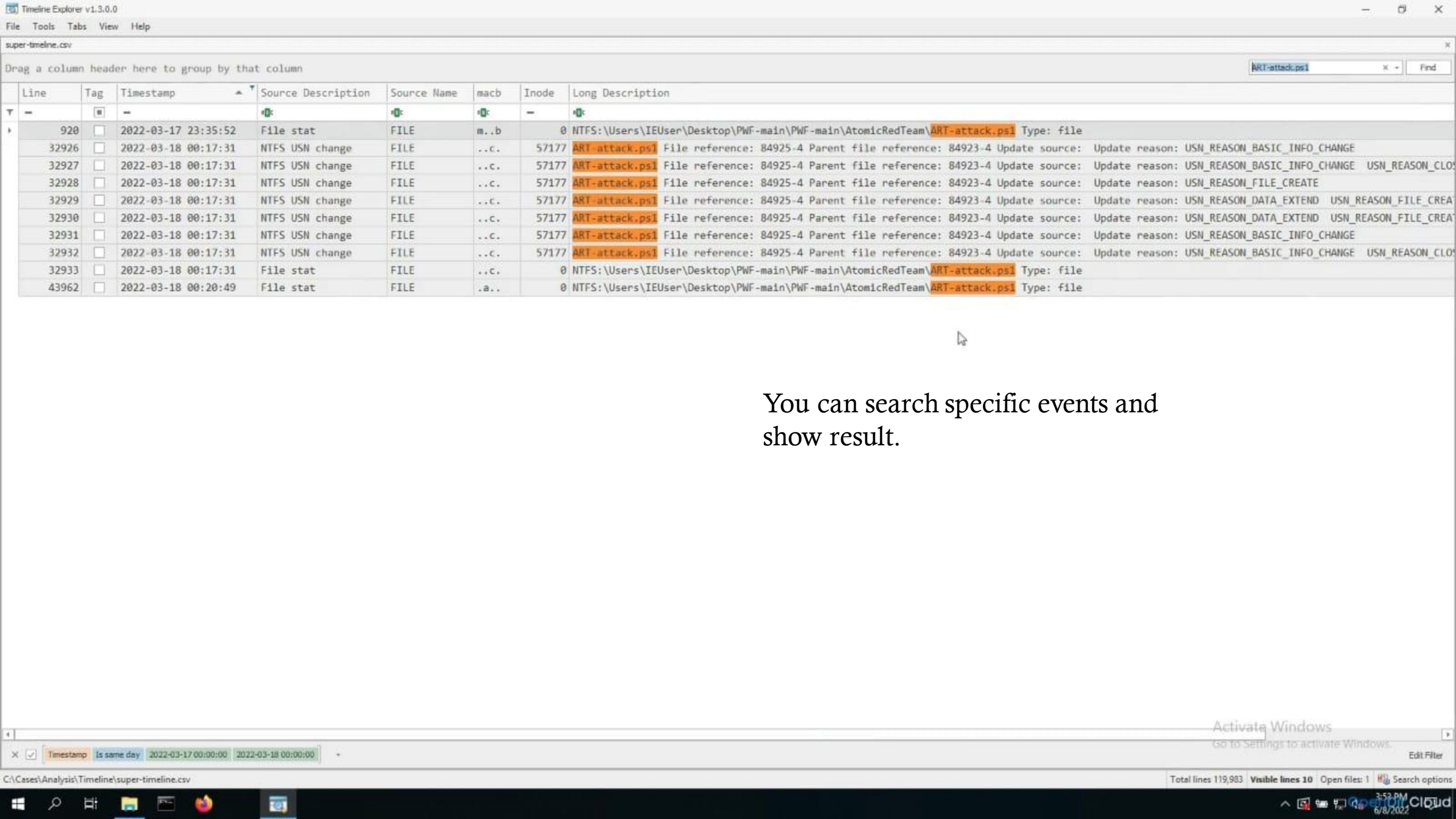
Total lines 119,983 Visible lines 119,983 Open files: 1 Search options


Timeline Explorer v1.3.0.0
File Tools Tabs View Help
super-timeline.csv
Drag a column header here to group by that column
Enter text to search...
Find
Line Tag Timestamp Source Description
Values Text Filters
Enter text to search...
(All)
Amcache Registry Entry
AppCompatCache Registry Entry
Background Activity 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
Clear Filter
Close
You can filter the specific events.
Activate Windows
Go to Settings to activate Windows.
C:\Cases\Analysis\Timeline\super-timeline.csv
Total lines 119,983 Visible lines 119,983 Open files: 1 Search options

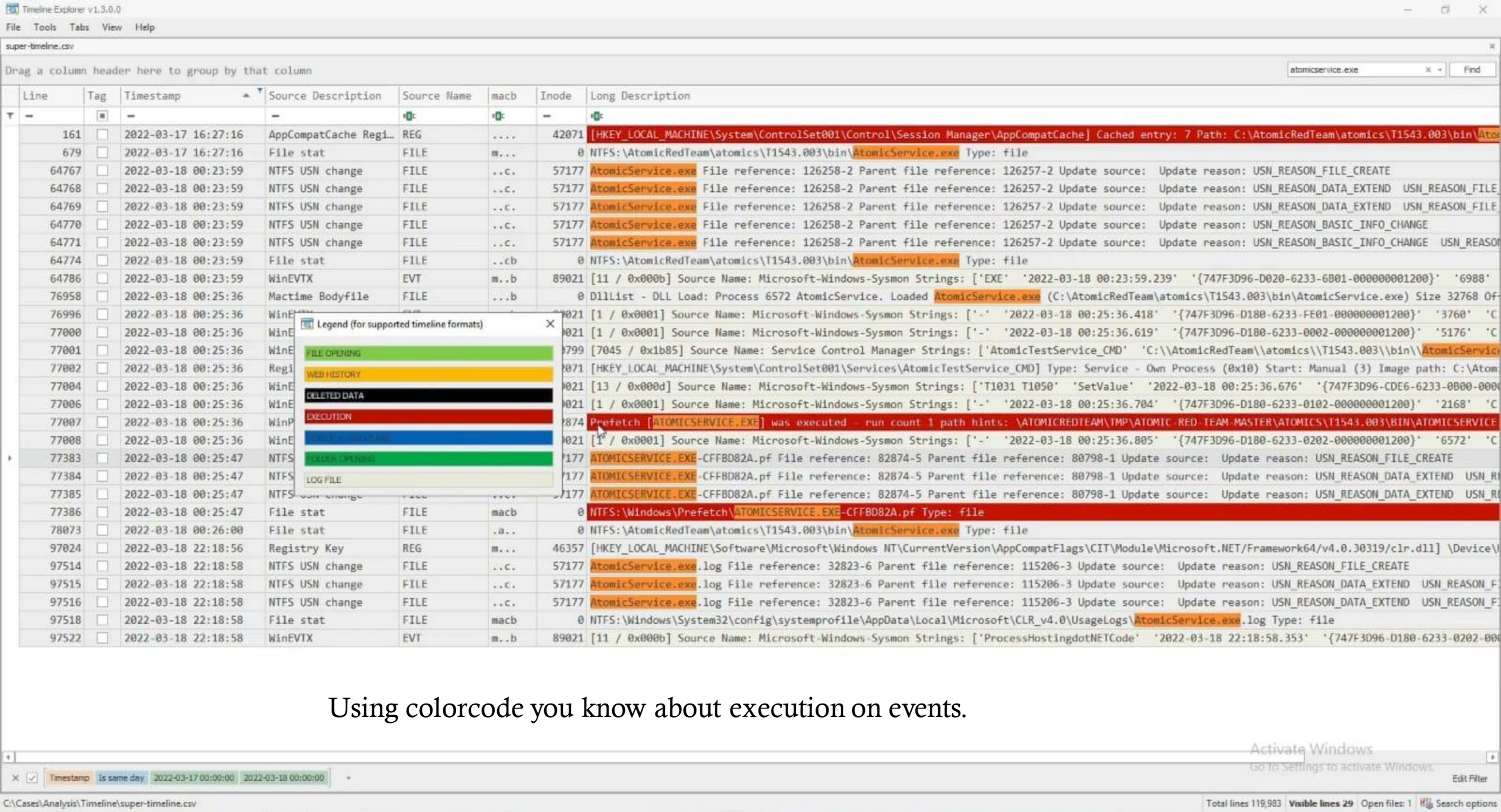
Super timeline Analysis Malicious Events



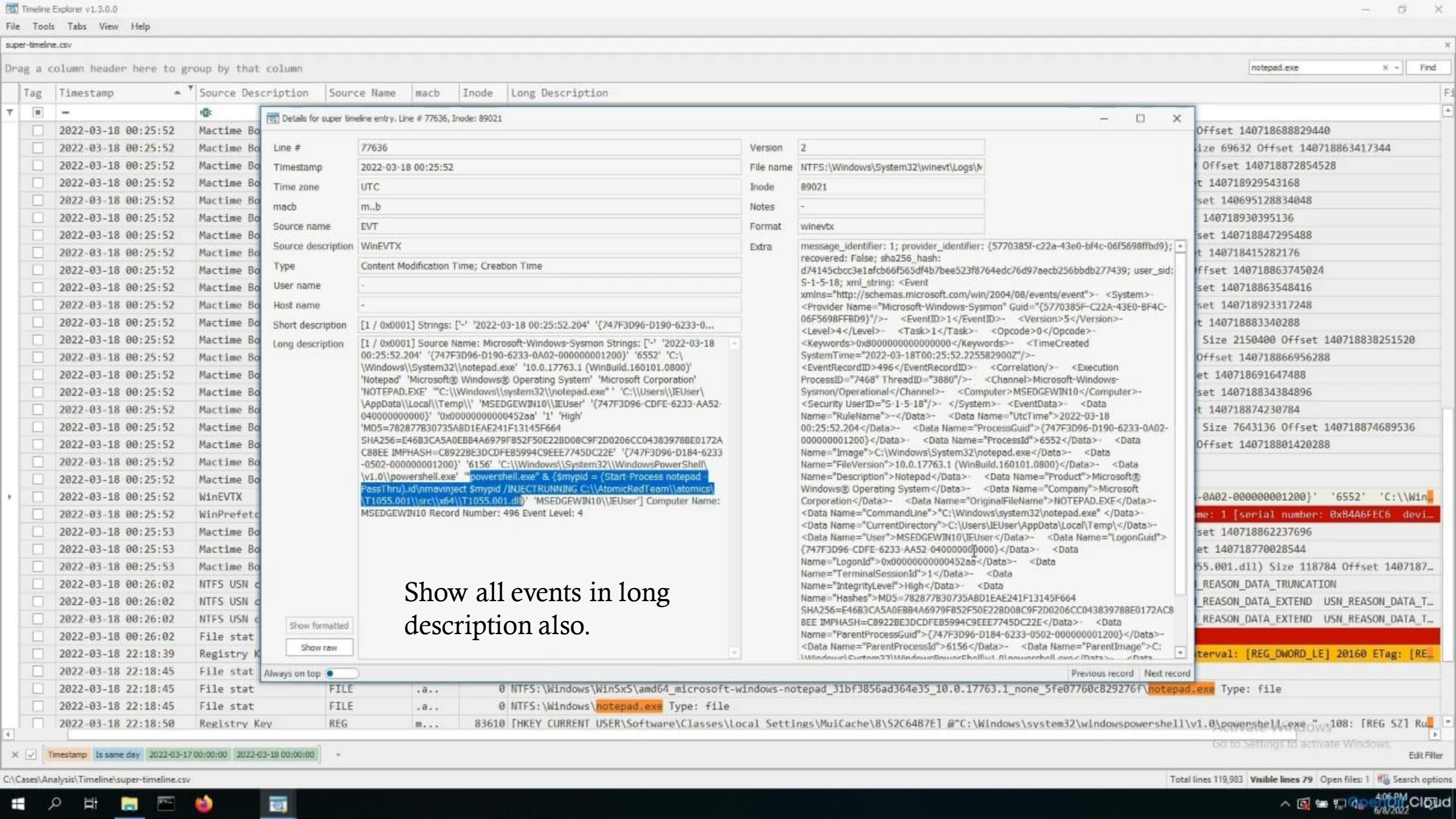
You can show all events



You can search specific events and show result.



Using colorcode you know about execution on 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
notepad.exe
Find
Tag Timestamp Source Description Source Name macb Inode Long Description
Details for super timeline entry. Line # 77636, Inode: 89021
Line # 77636
Timestamp 2022-03-18 00:25:52
Time zone UTC
macb m..b
Source name EVT
Source description WinEVTX
Type Content Modification Time; Creation Time
User name -
Host name -
Short description [1 / 0x0001] Strings: ['-' '2022-03-18 00:25:52.204' '{747F3D96-D190-6233-0...
Long description
[1 / 0x0001] Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2022-03-18 00:25:52.204' '{747F3D96-D190-6233-0A02-000000001200}' '6552' 'C:\\Windows\\System32\\notepad.exe' '10.0.17763.1 (WinBuild.160101.0800)' 'Notepad' 'Microsoft® Windows® Operating System' 'Microsoft Corporation' 'NOTEPAD.EXE' '"C:\\Windows\\system32\\notepad.exe" ' 'C:\\Users\\IEUser\\AppData\\Local\\Temp\\' 'MSEDGEWIN10\\IEUser' '{747F3D96-CDFE-6233-AA52-040000000000}' '0x00000000000452aa' '1' 'High' 'MD5=782877B30735ABD1EAE241F13145F664 SHA256=E46B3CA5A0EBB4A6979F852F50E22BD08C9F2D0206CC04383978BE0172AC88EE IMPHASH=C8922BE3DCDFEB5994C9EEE7745DC22E' '{747F3D96-D184-6233-0502-000000001200}' '6156' 'C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe' '"powershell.exe" & {$mypid = (Start-Process notepad -PassThru).id\nmavinject $mypid /INJECTRUNNING C:\\AtomicRedTeam\\atomics\\T1055.001\\src\\x64\\T1055.001.dll}' 'MSEDGEWIN10\\IEUser'] Computer Name: MSEDGEWIN10 Record Number: 496 Event Level: 4
Show formatted
Show raw
Always on top
Version 2
File name NTFS:\Windows\System32\winevt\Logs\M
Inode 89021
Notes -
Format winevtx
Extra
message_identifier: 1; provider_identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9}; recovered: False; sha256_hash: d74145cbcc3e1afcb66f565df4b7bee523f8764edc76d97aecb256bbdb277439; user_sid: S-1-5-18; xml_string: <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FFBD9}"/> <EventID>1</EventID> <Version>5</Version> <Level>4</Level> <Task>1</Task> <Opcode>0</Opcode> <Keywords>0x8000000000000000</Keywords> <TimeCreated SystemTime="2022-03-18T00:25:52.2255829002"/> <EventRecordID>496</EventRecordID> <Correlation/> <Execution ProcessID="7468" ThreadID="3880"/> <Channel>Microsoft-Windows-Sysmon/Operational</Channel> <Computer>MSEDGEWIN10</Computer> <Security UserID="S-1-5-18"/> </System> <EventData> <Data Name="RuleName"></Data> <Data Name="UtcTime">2022-03-18 00:25:52.204</Data> <Data Name="ProcessGuid">{747F3D96-D190-6233-0A02-000000001200}</Data> <Data Name="ProcessId">6552</Data> <Data Name="Image">C:\Windows\System32\notepad.exe</Data> <Data Name="FileVersion">10.0.17763.1 (WinBuild.160101.0800)</Data> <Data Name="Description">Notepad</Data> <Data Name="Product">Microsoft® Windows® Operating System</Data> <Data Name="Company">Microsoft Corporation</Data> <Data Name="OriginalFileName">NOTEPAD.EXE</Data> <Data Name="CommandLine">"C:\Windows\system32\notepad.exe" </Data> <Data Name="CurrentDirectory">C:\Users\IEUser\AppData\Local\Temp\</Data> <Data Name="User">MSEDGEWIN10\IEUser</Data> <Data Name="LogonGuid">{747F3D96-CDFE-6233-AA52-040000000000}</Data> <Data Name="LogonId">0x00000000000452aa</Data> <Data Name="TerminalSessionId">1</Data> <Data Name="IntegrityLevel">High</Data> <Data Name="Hashes">MD5=782877B30735ABD1EAE241F13145F664 SHA256=E46B3CA5A0EBB4A6979F852F50E22BD08C9F2D0206CC04383978BE0172AC88EE IMPHASH=C8922BE3DCDFEB5994C9EEE7745DC22E</Data> <Data Name="ParentProcessGuid">{747F3D96-D184-6233-0502-000000001200}</Data> <Data Name="ParentProcessId">6156</Data> <Data Name="ParentImage">C:
Previous record
Next record
Show all events in long description also.
2022-03-18 00:25:52 Mactime Bo
2022-03-18 00:25:52 WinEVTX
2022-03-18 00:25:53 Mactime Bo
2022-03-18 00:26:02 NTFS USN c
2022-03-18 00:26:02 File stat
2022-03-18 22:18:39 Registry K
2022-03-18 22:18:45 File stat FILE .a.. 0 NTFS:\Windows\WinSxS\amd64_microsoft-windows-notepad_31bf3856ad364e35_10.0.17763.1_none_5fe07760c829276f\notepad.exe Type: file
2022-03-18 22:18:45 File stat FILE .a.. 0 NTFS:\Windows\notepad.exe Type: file
2022-03-18 22:18:50 Registry Key REG m... 83610 [HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\8\52C6487E] @"C:\Windows\system32\windowspowershell\v1.0\powershell.exe" ,-108: [REG_SZ] Ru
Timestamp Is same day 2022-03-17 00:00:00 2022-03-18 00:00:00
Edit Filter
C:\Cases\Analysis\Timeline\super-timeline.csv
Total lines 119,983 Visible lines 79 Open files: 1 Search options

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